

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-177523

(43)Date of publication of application : 30.06.1998

(51)Int.Cl.	G06F 12/14
	G06F 12/00
	G06F 12/00
	G09C 1/00
	H04L 9/14

(21)Application number : 08-335594 (71)Applicant : MITSUBISHI ELECTRIC CORP

(22)Date of filing : 16.12.1996 (72)Inventor : FUJII SEIJI

(54) MULTIMEDIA INFORMATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To guarantee the execution of multimedia information to the user of a multimedia information system based on the terms of the contract made by the user by eliminating unauthorized access to the multimedia information.

SOLUTION: A multimedia information server 6 is provided with a ciphering system deciding means 8a which decides an enciphering means which enciphers multimedia information and a decoding means which decodes enciphered multimedia information based on the terms of the contract made by a user stored in a user information database 9 and a transmitting means 7 which enciphers the multimedia information stored in the database 10 by using the enciphering means decided by the means 8a and transmits the enciphered multimedia information and a multimedia client 1 is provided with a receiving means 4 which decodes the enciphered multimedia information transmitted from the transmitting means 7 by using the decoding means decided by the deciding means 8.

CLAIMS

[Claim(s)]

[Claim 1] A multimedia information system provided with the following elements.

(a) The User Information memory measure which memorizes contract information with a user;

(b) A multimedia information memory measure which memorizes multimedia information containing a character, a figure, a sound, still picture, sub-division or an animation;

(c) A server provided with the following elements;

(c1) A ciphering system deciding means which determines an encoding means which enciphers the above-mentioned multimedia information and a decoding means which decodes multimedia information enciphered by this encoding means based on the above-mentioned contract information memorized by the above-mentioned User Information memory measure;

(c2) A transmitting means which enciphers multimedia information memorized by the above-mentioned multimedia information memory measure using an encoding means determined by this ciphering system deciding means and transmits this enciphered multimedia information;

(d) A client which is provided with the following elements and requires transmission of the above-mentioned multimedia information of the above-mentioned server;

(d1) A reception means which decodes encryption multimedia information transmitted by the above-mentioned transmitting means using a decoding means determined by the above-mentioned ciphering system deciding means.

[Claim 2] Have a cipher system memory measure which memorizes two or more decoding means which decode data enciphered by two or more encoding means which perform encryption different respectively and each of this encoding means and the above-mentioned server. An encoding means and a decoding means which were determined by the above-mentioned ciphering system deciding means are taken out from the above-mentioned cipher system memory measure. Have a cipher system transmitting means which transmits this taken-out encoding means and decoding means and the above-mentioned transmitting means. The multimedia information system according to claim 1 enciphering using an encoding means transmitted by the above-mentioned cipher system transmitting means and decoding the above-mentioned reception means using a decoding means transmitted by the above-mentioned cipher system transmitting means.

[Claim 3] The above-mentioned transmitting means is provided with a cipher system memory measure which memorizes two or more encoding means which perform encryption different respectively. Take out an encoding means determined by the above-mentioned ciphering system deciding means from the above-mentioned cipher system memory measure and encipher using this taken-out encoding means and the above-mentioned reception means. It has a decode system memory measure which memorizes two or more decoding means which decode data enciphered by encoding means memorized by the above-mentioned cipher system memory measure. The multimedia information system according to claim 1 taking out a decoding means determined by the above-mentioned ciphering system deciding means from the above-mentioned decode system memory measure and decoding using this taken-out

decoding means.

[Claim 4] Have an area information memory measure which memorizes area information which shows an usable area of the above-mentioned encoding means and the above-mentioned ciphering system decoding means. The multimedia information system according to claim 1 characterized by determining the above-mentioned encoding means and the above-mentioned decoding means based on the above-mentioned area information memorized by the above-mentioned contract information memorized by the above-mentioned User Information memory measure and the above-mentioned area information memory measure.

[Claim 5] The multimedia information system comprising according to claim 1:

Two or more encryption execution means which perform an encoding means which enciphers multimedia information with which the above-mentioned ciphering system decoding means transmitted an encoding means and a decoding means which were newly determined and the above-mentioned transmitting means was remembered to be by the above-mentioned multimedia information memory measure.

A cipher system alteration means which makes the above-mentioned encryption execution means which is not under execution perform the new encoding means transmitted by the above-mentioned ciphering system decoding means.

Two or more decoding execution means which perform a decoding means which decodes encryption multimedia information which was equipped with a transmission control means which transmits multimedia information enciphered by the above-mentioned encryption execution means and to which the above-mentioned reception means was transmitted by the above-mentioned transmission control means.

A decode system alteration means which makes the above-mentioned decoding execution means which is not under execution perform the new decoding means transmitted by the above-mentioned ciphering system decoding means.

[Claim 6] The above-mentioned transmission control means builds send data which stored classification of an encoding means used in order to encipher as multimedia information enciphered by the above-mentioned encryption execution means and transmits. The above-mentioned decode system alteration means receives the above-mentioned send data and distinguishes an encoding means which enciphered the above-mentioned multimedia information based on the above-mentioned classification stored in this received data. The multimedia information system according to claim 5 making the above-mentioned decoding execution means perform a decoding means corresponding to this encoding means.

[Claim 7] A multimedia information system provided with the following elements.

(a) The User Information memory measure which memorizes contract information with a user;

(b) A multimedia information memory measure which memorizes multimedia information containing a character, a figure, a sound, Still Picture, Sub-Division, or an

animation;

(c) A server provided with the following elements;

(c1) A transmitting means which enciphers multimedia information memorized by the above-mentioned multimedia information memory measure and transmits this enciphered multimedia information;

(c2) Receive execution information of the above-mentioned multimedia information and contract information memorized by this execution information and the above-mentioned User Information memory measure is compared. A control means which distinguishes whether the above-mentioned multimedia information is performed based on the above-mentioned contract information and controls transmission of multimedia information by the above-mentioned transmitting means;

(d) A client which is provided with the following elements and requires transmission of the above-mentioned multimedia information of the above-mentioned server;

(d1) A reception means which decodes encryption multimedia information transmitted by the above-mentioned transmitting means;

(d2) An execution means which performs multimedia information decoded by this reception means;

(d3) An execution information transmitting means which transmits execution information which shows a state under execution of this execution means to the above-mentioned control means.

[Claim 8] The above-mentioned server is provided with an execution information transmission system determination means to determine a transmission system of the above-mentioned execution information by the above-mentioned execution information transmitting means based on contract information memorized by the above-mentioned User Information memory measure. The multimedia information system according to claim 7 wherein the above-mentioned execution information transmitting means transmits the above-mentioned execution information with a transmission system determined by the above-mentioned execution information transmission system determination means.

[Claim 9] Memorize the above-mentioned User Information memory measure and contract information with a user and execution control information over multimedia information the above-mentioned control means. Execution information which received [above-mentioned] is compared with contract information and execution control information which were memorized by the above-mentioned User Information memory measure. The multimedia information system according to claim 7 distinguishing whether the above-mentioned multimedia information is performed based on the above-mentioned contract information and the above-mentioned execution control information and controlling transmission of the above-mentioned multimedia information.

[Claim 10] Memorize the above-mentioned multimedia information memory measure and execution constraints which restrain execution of the above-mentioned

multimedia information and this multimedia information the above-mentioned control meansContract information memorized by the above-mentioned User Information memory measure in execution information which received [above-mentioned]And it compares with execution constraints memorized by the above-mentioned multimedia information memory measureThe multimedia information system according to claim 7 distinguishing whether the above-mentioned multimedia information is performed based on the above-mentioned contract information and the above-mentioned execution constraintsand controlling transmission of the above-mentioned multimedia information.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention relates to the multimedia information system which enciphers and provides the user who contracted with the multimedia information which consists of a charactera figurea soundStill Picture Sub-Divisionor an animation.

[0002]

[Description of the Prior Art]Drawing 20 is an outline block diagram showing the conventional multimedia information system shownfor example in JPH6-44122A. The multimedia information accumulating part which 50 enciphers the multimedia file which consists of various-media data of a charactera figurea soundStill Picture Sub-Divisionan animationetc.and is accumulated in a figureThe multimedia information Management Department which manages input and output of a multimedia file [as opposed to the multimedia information accumulating part 50 in 51]and 52 are output units which display the contents of the multimedia file.

[0003]Drawing 21 is a block diagram of the media data which is a component of the multimedia file accumulated in the multimedia information accumulating part 50. The enciphering key information for 60 responding to media dataand 60a responding to a user's security leveland distinguishing whether it is accessible data in a figureThe position and size information 60b indicates the display position and the size to display on a display screen to beThe media kind information 60c indicates the media classification of media data to beand 60 d are the output unit associated data which added the data of the data format different from the time of an input for the correspondence to the display screen from which presentation capability differs. Thusit has the enciphering key information for distinguishing whether access by a user is possible for every media dataand a security level can be changed by each media data unit which constitutes the multimedia file.

[0004]Nextoperation is explained. If a user makes demands on the multimedia

information Management Department 51 for the output of a multimedia file the multimedia information Management Department 51 will take out the media data 60 which constitutes the multimedia file with an output request from the multimedia information accumulating part 50. Next the multimedia information Management Department 51 analyzes a user's security level and distinguishes whether it is accessible media data with the user's security level based on the enciphering key information 60a included in each media data 60. And when a user distinguishes that it is accessible media data only this accessible media data 60 is set as the object of an output and it changes into the data format according to the presentation capability of the output unit 52 and outputs to the output unit 52.

[0005]

[Problem to be solved by the invention] The conventional multimedia information system is constituted as mentioned above accumulated the enciphered multimedia information and has transmitted to the user. Therefore since the same cipher system will be used over a long period of time common data is intercepted by third parties other than the user who has contracted and the cipher system was decoded there was a problem that a third party could access unjustly to the multimedia information transmitted to the user.

[0006] Before transmitting multimedia information only check conditions of contract about execution of a user's multimedia information and during execution of multimedia information Since it was not able to be confirmed whether a user is performing correctly based on conditions of contract there was a problem that multimedia information will be able to be performed unjustly.

[0007] There was a problem that execution of multimedia information according to conditions of contract about execution of multimedia information of various users such as execution of multimedia information by time and a time basis and execution frequency was uncontrollable.

[0008] This invention is made in order to cancel the above problems and it eliminates unjust access to multimedia information by a third party and an object of invention is to obtain a multimedia information system which guarantees that a user performs multimedia information based on conditions of contract.

[0009]

[Means for solving problem] The multimedia information system according to claim 1 is provided with the following elements.

- (a) The User Information memory measure which memorizes contract information with a user;
- (b) A multimedia information memory measure which memorizes multimedia information containing a character a figure a sound Still Picture Sub-Division or an animation;
- (c) A server provided with the following elements;
- (c1) A ciphering system deciding means which determines an encoding means which

enciphers the above-mentioned multimedia information and a decoding means which decodes multimedia information enciphered by this encoding means based on the above-mentioned contract information memorized by the above-mentioned User Information memory measure;

(c2) A transmitting means which enciphers multimedia information memorized by the above-mentioned multimedia information memory measure using an encoding means determined by this ciphering system deciding means and transmits this enciphered multimedia information;

(d) A client which is provided with the following elements and requires transmission of the above-mentioned multimedia information of the above-mentioned server;

(d1) A reception means which decodes encryption multimedia information transmitted by the above-mentioned transmitting means using a decoding means determined by the above-mentioned ciphering system deciding means.

[0010] The multimedia information system according to claim 2 has a cipher system memory measure which memorizes two or more decoding means which decode data enciphered by two or more encoding means which perform encryption different respectively and each of this encoding means and the above-mentioned server. An encoding means and a decoding means which were determined by the above-mentioned ciphering system deciding means are taken out from the above-mentioned cipher system memory measure. It has a cipher system transmitting means which transmits this taken-out encoding means and decoding means. The above-mentioned transmitting means is enciphered using an encoding means transmitted by the above-mentioned cipher system transmitting means and the above-mentioned reception means is decoded using a decoding means transmitted by the above-mentioned cipher system transmitting means.

[0011] The multimedia information system according to claim 3 has a cipher system memory measure which memorizes two or more encoding means which perform encryption different respectively. The transmitting means which takes out the encoding means determined by the above-mentioned ciphering system deciding means from the above-mentioned cipher system memory measure and is enciphered using this taken-out encoding means. It has a decode system memory measure which memorizes two or more decoding means which decode the data enciphered by the encoding means memorized by the above-mentioned cipher system memory measure. The decoding means determined by the above-mentioned ciphering system deciding means is taken out from the above-mentioned decode system memory measure and it has a reception means decoded using this taken-out decoding means.

[0012] The multimedia information system according to claim 4 has an area information memory measure which memorizes the area information which shows the usable area of the above-mentioned encoding means and the above-mentioned ciphering system deciding means. Based on the above-mentioned area information memorized by the above-mentioned contract information memorized by the above-

mentioned User Information memory measure and the above-mentioned area information memory measure the above-mentioned encoding means and the above-mentioned decoding means are determined.

[0013] The multimedia information system according to claim 5 has a ciphering system deciding means which transmits the newly determined encoding means and a decoding means and the above-mentioned transmitting means. Two or more encryption execution means which perform the encoding means which enciphers the multimedia information memorized by the above-mentioned multimedia information memory measure. The cipher system alteration means which makes the above-mentioned encryption execution means which is not under execution perform the new encoding means transmitted by the above-mentioned ciphering system deciding means. Have a transmission control means which transmits the multimedia information enciphered by the above-mentioned encryption execution means and the above-mentioned reception means. It has two or more decoding execution means which perform the decoding means which decodes the encryption multimedia information transmitted by the above-mentioned transmission control means and a decode system alteration means which makes the above-mentioned decoding execution means which is not under execution perform the new decoding means transmitted by the above-mentioned ciphering system deciding means.

[0014] The multimedia information system according to claim 6A transmission control means which builds send data which stored classification of an encoding means used in order to encipher as multimedia information enciphered by the above-mentioned encryption execution means and transmits. The above-mentioned send data is received and an encoding means which enciphered the above-mentioned multimedia information based on the above-mentioned classification stored in this received data is distinguished and it has a decode system alteration means which makes the above-mentioned decoding execution means perform a decoding means corresponding to this encoding means.

[0015] The multimedia information system according to claim 7 is provided with the following elements.

- (a) The User Information memory measure which memorizes contract information with a user;
- (b) A multimedia information memory measure which memorizes multimedia information containing a character, a figure, a sound, Still Picture, Sub-Division or an animation;
- (c) A server provided with the following elements;
 - (c1) A transmitting means which enciphers multimedia information memorized by the above-mentioned multimedia information memory measure and transmits this enciphered multimedia information;
 - (c2) Receive execution information of the above-mentioned multimedia information and contract information memorized by this execution information and the

above-mentioned User Information memory measure is comparedA control means which distinguishes whether the above-mentioned multimedia information is performed based on the above-mentioned contract informationand controls transmission of multimedia information by the above-mentioned transmitting means;

(d) Client which is provided with the following elements and requires transmission of the above-mentioned multimedia information of the above-mentioned server;

(d1) Reception means which decodes the encryption multimedia information transmitted by the above-mentioned transmitting means;

(d2) Execution means which performs multimedia information decoded by this reception means;

(d3) The execution information transmitting means which transmits the execution information which shows the state under execution of this execution means to the above-mentioned control means.

[0016]The multimedia information system according to claim 8The above-mentioned server is equipped with an execution information transmission system determination means to determine the transmission system of the above-mentioned execution information by the above-mentioned execution information transmitting means based on the contract information memorized by the above-mentioned User Information memory measureThe above-mentioned execution information transmitting means transmits the above-mentioned execution information with the transmission system determined by the above-mentioned execution information transmission system determination means.

[0017]The multimedia information system according to claim 9The User Information memory measure which memorizes contract information with a userand the execution control information over multimedia informationThe execution information which received [above-mentioned] is compared with the contract information and the execution control information which were memorized by the above-mentioned User Information memory measureIt distinguishes whether the above-mentioned multimedia information is performed based on the above-mentioned contract information and the above-mentioned execution control informationand has a control means which controls transmission of the above-mentioned multimedia information.

[0018]The multimedia information system according to claim 10A multimedia information memory measure which memorizes execution constraints which restrain execution of the above-mentioned multimedia information and this multimedia informationContract information memorized by the above-mentioned User Information memory measure in execution information which received [above-mentioned]And it compares with execution constraints memorized by the above-mentioned multimedia information memory measuredistinguishes whether the above-mentioned multimedia information is performed based on the above-mentioned contract information and the above-mentioned execution constraintsand has a control means which controls transmission of the above-mentioned multimedia information.

[0019]

[Mode for carrying out the invention]

Below embodiment 1. explains this invention referring to a figure based on an embodiment. Drawing 1 is a block diagram of a multimedia information system of Embodiment 1. In a figure while a multimedia client as which 1 requires transmission of multimedia information and 2 receive a demand from a user An input output means which outputs an executed result of multimedia information and 3 perform multimedia information An execution control means to transmit an executed result to the input output means 2 and 4 receive and decode enciphered multimedia information A network and 6 a reception means which transmits to the execution control means 3 and 5 A multimedia information server While a transmitting means which 7 enciphers multimedia information and transmits to the multimedia client 1 via the network 5 and 8 determine a cipher system A user information data base as an information control means which controls transmission of multimedia information and a User Information memory measure which is accumulating contract information of all the users who have made a contract of 9 A multimedia information database as a multimedia information memory measure for which 10 is accumulating all the multimedia information for which the multimedia information server 6 provides service 11 is a cipher system database as a cipher system memory measure which is accumulating a key generating means an encoding means and a decoding means of all the cipher systems which can be used by the multimedia information server 6.

[0020] The information control means 8 comprises the ciphering system deciding means 8a the cipher system transmitting means 8b and the key generation part 8c. The ciphering system deciding means 8a determines a cipher system used when transmitting multimedia information based on a user's contract information accumulated in the user information data base 9. The cipher system transmitting means 8b takes out a key generating means an encoding means and a decoding means of a cipher system determined by the ciphering system deciding means 8a from the cipher system database 11 a key generating means transmits to the key generation part 8c an encoding means transmits to the transmitting means 7 and a decoding means transmits it to the reception means 4. The key generation part 8c generates an enciphering key and a decode key using a key generating means transmitted by the cipher system transmitting means 8b.

[0021] As illustrated this system the multimedia information server 6 and two or more multimedia clients 1 It is connected to the network 5 and the multimedia information server 6 takes out multimedia information demanded from the multimedia client 1 from the multimedia information database 10 enciphers and transmits to the multimedia client 1.

[0022] Drawing 2 is a block diagram showing composition of contract information accumulated in the user information data base 9. As for a contract information record with a user and 9b in a figure 9a is [a user's address and 9e of a user registration

number and 9c (a user's name and 9 d)] a contract type with a user. The contract type 9e is the information for determining a cipher system.

[0023]Drawing 3 is a block diagram showing composition of multimedia information accumulated in the multimedia information database 10. In a figure a real whereabouts type number which a multimedia information number to identify 10a on a multimedia information record and for 10b identify multimedia information uniquely and 10c show a name of multimedia information and shows 10 d of execution means of multimedia information and 10 f are multimedia information.

[0024]Drawing 4 is a block diagram showing composition of a cipher system accumulated in the cipher system database 11. A cipher system number to identify 11a on a cipher system record and for 11b identify a cipher system uniquely in a figure A key generating means which 11c generates a name of a cipher system and generates 11 d of enciphering keys and decode keys an encoding means as which 11e enciphers multimedia information and 11 f are decoding means which decode enciphered multimedia information.

[0025] Next it explains based on the flow chart of ***** of operation and drawing 5. Out of the multimedia information number 10a and the multimedia information name 10c which are displayed on the input output means 2. When a user chooses the one multimedia information number 10a (Step S1) the execution control means 3 The user registration number 9b inputted by the user and the selected multimedia information number 10a are transmitted to the cipher system transmitting means 8b of the multimedia information server 6 (Step S2). The cipher system transmitting means 8b outputs the user registration number 9b to the ciphering system deciding means 8a (Step S3).

[0026] The ciphering system deciding means 8a acquires a user's contract information record 9a from the user information data base 9 by making the user registration number 9b into a search condition (step S4) The cipher system number 11b of the cipher system which determined and determined the cipher system based on the contract type 9e in the acquired contract information record 9a is outputted to the cipher system transmitting means 8b (Step S5).

[0027] The cipher system transmitting means 8b acquires the key generating means 11d the encoding means 11e and the decoding means 11f from the cipher system database 11 by making the cipher system number 11b into a search condition (Step S6). The cipher system transmitting means 8b outputs the key generating means 11d to the key generation part 8c (Step S7) and the key generation part 8c uses this outputted key generating means 11d and generates an enciphering key and a decode key and it outputs it to the cipher system transmitting means 8b (Step S8). The enciphering key with which the cipher system transmitting means 8b was generated by the key generation part 8c The encoding means 11e acquired from the cipher system database 11 is outputted to the transmitting means 7 (step S9) and the decode key generated by the key generation part 8c and the decoding means 11f

acquired from the cipher system database 11 are transmitted to the reception means 4 (Step S10).

[0028]Nextthe cipher system transmitting means 8b makes a search condition the multimedia information number 10a transmitted at Step S2 and10 f of multimedia information which the user chose is taken out from the multimedia information database 10and it divides into a blockand outputs to the transmitting means 7 (Step S11). Using the enciphering key and the encoding means 11e which were outputted by step S9the transmitting means 7 enciphers each block of 10 f of multimedia informationand transmits to the reception means 4 (Step S12).

[0029]The reception means 4 decodes each block of 10 f of received encryption multimedia information using a decode key and the decoding means 11f to which it was transmitted at Step S10and transmits to the execution control means 3 (Step S13). The execution control means 3 performs 10 f of decoded multimedia informationand outputs an executed result to the input output means 2 (Step S14).

[0030]As mentioned abovesince according to this embodiment a cipher system was chosen based on a user's contract type and a cipher system is changed for every user out of a cipher system of a large number accumulated in the cipher system database 11Since a guess of a cipher system is difficult for a third partyit is effective in the ability to eliminate unjust access.

[0031]Although the ciphering system deciding means 8a determined a cipher system and a form to which the cipher system transmitting means 8b transmits a key generating meansand a decoding means was shown by this embodimentit can also constitute so that the ciphering system deciding means 8a may have a function of the cipher system transmitting means 8b and may transmit each means corresponding to a determined cipher system.

[0032]When neither an encoding means performed by the embodiment 2. transmitting means 7 nor a decoding means performed by the reception means 4 can be changedAs shown in drawing 6a multimedia information system is also realizable from the information control means 8 changing the transmitting means 7and ordering and changing using several different transmitting means 7 and reception means 4 of a cipher systemso that the reception means 4 of the same cipher system may be used to the execution control means 3.

[0033]When transmitting the decoding means 11f via embodiment 3. and a networkin order to shorten that the decoding means 11f may be stolen by the third party and time to transmit the decoding means 11f to the reception means 4As shown in drawing 7the decoding means database 12 which accumulated only the decoding means in the multimedia client side can also be distributed and arranged.

[0034]In an embodiment 4. panas shown in drawing 8it can also constitute so that the transmitting means 7 by the side of a multimedia information server may have the encoding means database 13 and the reception means 4 of a multimedia client side may have the decoding means database 12 in an inside.

[0035]According to the embodiment 5, embodiment 1 although the cipher system was determined based on the contract type in contract information with a user when two or more candidates of the cipher system corresponding to a contract type remain in order to determine a cipher system as one information other than a contract type is needed.

[0036]When transmitting and receiving the data enciphered between the user and the multimedia information server, a usable cipher system may be restricted by the law of an inhabitable area. Since the same cipher system cannot necessarily be used at all in the area where a multimedia client exists with an usable cipher system and a cipher system usable in the area where a multimedia information server exists, it is necessary to determine the cipher system which can be used at both places but and. This cannot be judged only by conditions of contract with a user individual. So a cipher system database is made into the structure shown in drawing 9 in this embodiment. The cipher system database shown in drawing 9 adds 11 g of usable area information which shows the usable area of each cipher system to the cipher system database shown in drawing 4.

[0037]Although the composition of the multimedia information system of this embodiment is the same as the composition of drawing 1 explained by Embodiment 1, operation of the cipher system determination in the ciphering system deciding means 8a differs from the thing of Embodiment 1. Different operations are step S4 explained by Embodiment 1 and S5. Different operation is explained below. According to this embodiment, the ciphering system deciding means 8a acquires a user's contract information record 9a from the user information data base 9 by making the user registration number 9b into a search condition. Next, the cipher system record 11a is picked out from the cipher system database 11 shown in drawing 8. And 9 d of addresses in the acquired contract information record 9a investigate whether it agrees in 11 g of usable area information in the cipher system record 11a. When the agreeing cipher system is plurality, the cipher system which agrees from the inside in the contract type 9e in a user's contract information record 9a is determined and the cipher system number 11b of the determined cipher system is outputted to the cipher system transmitting means 8b.

[0038]As mentioned above, a cipher system can be chosen also when the cipher system which can be used changes with area, since a cipher system is determined based on a user's contract type and the usable area information of a cipher system according to this embodiment.

[0039]Embodiment 6, drawing 10 is a block diagram of the multimedia information system of Embodiment 6. In a figure, the execution control means 3 and the reception means 4 constitute a multimedia client like what was shown in drawing 1 and the transmitting means 7 and the information control means 8 constitute a multimedia information server like what was shown in drawing 1.

[0040]In the information control means 8, the ciphering system deciding means 8a, When

a cipher system is changed newly determine a cipher system and the cipher system transmitting means 8b. Taking out a key generating means and an encoding means and a decoding means from the cipher system database 11 shown in drawing 1 based on a new cipher system a key generating means transmits to the key generation part 8a. An encoding means transmits to the transmitting means 7 and a decoding means transmits to the reception means 4. The transmitting means 7 comprises the cipher system alteration means 7a, the encryption execution means 7b and 7c, and the transmission control means 7d. The cipher system alteration means 7a changes the encryption execution means 7b and 7c used by the transmitting means 7 based on the new encoding means transmitted by the cipher system transmitting means 8b. The encryption execution means 7b and 7c perform the encoding means transmitted from the cipher system transmitting means 8b, encipher the data outputted from the transmission control means 7d, and output the result to the transmission control means 7d. The transmission control means 7d outputs the block of the multimedia information outputted from the information control means 8 to the encryption execution means 7b or 7c and transmits the multimedia information enciphered by the encryption execution means 7b and 7c to the reception means 4.

[0041] The reception means 4 comprises the decode system alteration means 4a, the decoding execution means 4b and 4c, and the reception control means 4d. The decode system alteration means 4a changes the decoding execution means 4b and 4c used by the reception means 4 based on the new decoding means transmitted by the cipher system transmitting means 8b. The decoding execution means 4b and 4c perform the decoding means transmitted from the cipher system transmitting means 8b, decode the data outputted from the reception control means 4d, and output the result to the reception control means 4d. The reception control means 4d outputs the encryption multimedia information outputted from the transmission control means 7d to the decoding execution means 4b or 4c and transmits the multimedia information decoded by the decoding execution means 4b and 4c to the execution control means 3.

[0042] Next operation is explained based on the flow chart of drawing 11. The cipher system transmitting means 8b transmits the enciphering key and encoding means which were determined by the ciphering system deciding means 8a to the cipher system alteration means 7a (Step S20). The cipher system alteration means 7a outputs the enciphering key and encoding means which were received to the encryption execution means 7b and sets them up to encipher using the encryption execution means 7b (Step S21). The cipher system transmitting means 8b transmits to the decode system alteration means 4a a decode key and the decoding means reception means 4 (Step S22). The decode system alteration means 4a outputs the decode key and decoding means which were received to the decoding execution means 4b and sets them up to decode using the decoding execution means 4b (Step S23).

[0043] The information control means 8 divides multimedia information into a block and

transmits a block to the transmission control means 7d (Step S24). The transmission control means 7d outputs the received block to the encryption execution means 7b (Step S25). The encryption execution means 7b enciphers a block using the enciphering key and encoding means which were outputted at Step S21 and outputs it to the transmission control means 7d (Step S26). The transmission control means 7d transmits the enciphered block to the reception control means 4d via the network 5 (Step S27).

[0044]The reception control means 4d will be outputted to the decoding execution means 4b if the block of the multimedia information enciphered from the network 5 is received (Step S28). The decoding execution means 4b decodes an encryption block using the decode key and decoding means which were outputted at Step S23 and outputs it to the reception control means 4d (Step S29). The reception control means 4d transmits the decoded block to the execution control means 3 (Step S30).

[0045]Next the operation in the case of changing a cipher system is explained based on the flow chart of drawing 12 during execution of multimedia information. The information control means 8 will suspend transmission to the transmission control means 7d of a block of multimedia information if the cipher system used now is changed (Step S40). The cipher system transmitting means 8b transmits the enciphering key and encoding means after change for which it opted by the ciphering system deciding means 8a to the cipher system alteration means 7a (Step S41). The cipher system alteration means 7a outputs the enciphering key and encoding means which were received to the encryption execution means 7c and the block received next is set up encipher using the encryption execution means 7c (Step S42). The cipher system transmitting means 8b transmits the decode key and decoding means after change for which it opted by the ciphering system deciding means 8a to the decode system alteration means 4a (Step S43). The decode system alteration means 4a outputs the decode key and decoding means which were received to the decoding execution means 4c and the encryption block received next is set up decode using the decoding execution means 4c (Step S44).

[0046]The information control means 8 cancels a stop of transmission and divides multimedia information into a block and resumes transmission of a block to the transmission control means 7d (Step S45). The transmission control means 7d outputs a received block to the encryption execution means 7c (Step S46). The encryption execution means 7c enciphers ***** and a block and outputs an enciphering key and an encoding means after change outputted at Step S42 to the transmission control means 7d (Step S47). The transmission control means 7d transmits an enciphered block to the reception control means 4d via the network 5 (Step S48).

[0047]The reception control means 4d will be outputted to the decoding execution means 4c if a block of multimedia information enciphered from the network 5 is received (Step S49). A decode key and a decoding means which were outputted at

Step S42 are used for the decoding execution means 4c it decodes a block and outputs it to the reception control means 4d (Step S50). The reception control means 4d transmits a decoded block to the execution control means 3 (Step S51).

[0048] As mentioned above, since a cipher system to be used can be changed dynamically according to this embodiment when adding a cipher system to a multimedia information server, it is effective in that there is no necessity of changing hardware which constitutes a system.

[0049] Although the ciphering system deciding means 8a determines a new cipher system and the cipher system transmitting means 8b shows the form which transmits a key generating means, an encoding means, and a decoding means by this embodiment based on a new cipher system. The ciphering system deciding means 8a has a function of the cipher system transmitting means 8b and it can also constitute so that each means corresponding to a new cipher system may be transmitted.

[0050] In this embodiment as shown in drawing 10, the encryption execution means 7b and 7c within the transmitting means 7 and the decoding execution means 4b and 4c within the reception means 4 may be not only two but two or more. When the cipher system used once is saved at the encryption execution means 7b and 7c and the decoding execution means 4b and 4c and the same cipher system is used again, a new enciphering key is outputted to the encryption execution means 7b and 7c, a new decode key is outputted to the decoding execution means 4b and 4c, and the reuse of the encryption execution means 7b, the encoding means in 7c, and the decoding execution means 4b and the decoding means in 4c is carried out.

[0051] When the encryption execution means 7b and 7c or the decoding execution means 4b and 4c are already in use and there is nothing intact, it controls to use the low encryption execution means 7b and 7c or the decoding execution means 4b and 4c of frequency in use.

[0052] The embodiment 7. embodiment 7 creates the send data 14 constituted by the block of the enciphered multimedia information 14b and the cipher system number 14a of the cipher system used for the encryption as shown in drawing 13. Although the composition of a system is the same as that of the thing of drawing 10 explained by Embodiment 6, processes of the transmission control means 7d and the reception control means 4d differ. The reception control means 4d which the transmission control means 7d created the send data shown in drawing 13 transmitted to the reception control means 4d via the network 5 and received this. The cipher system number 14a determines the decoding means which decodes the enciphered multimedia information 14b and either the decoding execution means 4b or the decoding execution means 4c is made to perform decoding.

[0053] Embodiment 8. drawing 14 is a block diagram of the multimedia information system of Embodiment 8. In a figure 15 is a real whereabouts type database which is accumulating two or more means for performing multimedia information with the real whereabouts type number. The user information data base 9 is shown in drawing 2 and

shows drawing 3 the multimedia information database 10. The execution control means 3 comprises the execution information control means 3a and the execution means 3b. The execution means 3b performs multimedia information decoded by the reception means 4 and transmits an executed result to the input output means 2. The execution information control means 3a is a certain time interval and transmits execution information when performing multimedia information and a user's demand outputted by the input output means 2 to the multimedia information server 6. The accumulated time of execution of the user registration number 9b, the multimedia information number 10b under execution and the multimedia information by the present is included in execution information. The information control means 8 comprises the control means 8d and the multimedia information transmitting means 8e. The control means 8d receives the execution information of the multimedia information transmitted by the execution information control means 3a and analyzes the information and controls the multimedia information transmitting means 8e. The multimedia information transmitting means 8e acquires multimedia information from the multimedia information database 10 and transmits to the transmitting means 7. The transmitting means 7 enciphers multimedia information and transmits to the reception means 4.

[0054] Next operation until it starts execution of multimedia information is explained based on the flow chart of drawing 15. If a user chooses one multimedia information, the execution information control means 3a will transmit the user registration number 9b and the multimedia information number 10b to the control means 8d (Step S60). The control means 8d picks out a user's contract information record 9a from the user information data base 9 by making the user registration number 9b into a search condition. It is judged whether execution can be started at the time which could perform multimedia information with a demand from the contract type 9e or the demand suited (Step S61). If the control means 8d judges with the execution start of multimedia information being possible, it will pick out the multimedia information record 10a from the multimedia information database 10 by making the multimedia information number 10b into a search condition and will acquire 10d of real whereabouts type numbers (Step S62). Next, the control means 8d takes out an execution means from the real whereabouts type database 15 by making 10d of real whereabouts type numbers into a search condition and transmits to the execution information control means 3a (Step S63). The execution information control means 3a outputs the received execution means to the execution means 3b (Step S64). The control means 8d outputs the multimedia information number 10b to the multimedia information transmitting means 8e (Step S65). The multimedia information transmitting means 8e picks out the multimedia information record 10a from the multimedia information database 10 by making the multimedia information number 10b into a search condition, divides it into a block and transmits to the transmitting means 7 (Step S66).

[0055]The transmitting means 7 enciphers a received block and transmits to the reception means 4 via the network 5 (Step S67). The reception means 4 decodes a received block and transmits to the execution means 3b (Step S68). The execution means 3b outputs a message which execution preparation ended to the input output means 2 (Step S69). A user inputs an execution start of multimedia information from the input means 2 (Step S70). If directions of an execution start are received the execution information control means 3a will transmit a message of a start of execution of multimedia information to the control means 8d and will start calculation of accumulated time of execution (Step S71). The control means 8d will output a transmission start message to the multimedia information transmitting means 8e if a message of a start of execution of multimedia information is received (Step S72).

[0056]Next operation under execution of multimedia information is explained based on a flow chart of drawing 16. The multimedia information transmitting means 8e takes out multimedia information from the multimedia information database 10 by making the multimedia information number 10b into a search condition divides it into a block and transmits to the transmitting means 7 (Step S80). The control means 8d starts calculation of accumulated time of execution of multimedia information and waits for reception of execution information (Step S81). The transmitting means 7 enciphers a block of multimedia information and transmits to the reception means 4 via the network 5 (Step S82). The reception means 4 decodes a received block and transmits to the execution means 3b (Step S83). If multimedia information is received from the reception means 4 the execution means 3b will perform multimedia information and will output an executed result to the input output means 2 (Step S84).

[0057]If fixed time passes when having repeated operation of Steps S80–S84 (Step S85) the execution information control means 3a will transmit the execution information which set the accumulated time of execution of the multimedia information by the present to the control means 8d (Step S86). The control means 8d calculates the absolute value of the difference of the accumulated time of the execution which the control means 8d calculated and the accumulated time set to execution information. It is confirmed whether the absolute value of the difference is over the range of the error which the control means 8d holds (Step S87). When having exceeded it judges that the unjust execution which is not in agreement with (Step S88) and the contract type 9e was detected and the message which shows the stop of transmission is outputted to the multimedia information transmitting means 8e (Step S88). The multimedia information transmitting means 8e stops transmission of multimedia information (Step S89).

[0058]As mentioned above since according to this embodiment transmission is suspended when the execution accumulated time of multimedia information is checked based on a contract type and it is over predetermined time The effect of preventing execution of the unjust multimedia information which breaks conditions of contract is during execution of multimedia information.

[0059]Embodiment 9. drawing 17 is a block diagram of a multimedia information system of Embodiment 9. In a figure 8 f is an execution information transmission system determination means to determine timing which transmits execution information from the execution information control means 3a by demand from the control means 8d.

[0060]Next operation is explained. If a user chooses one multimedia information the execution information control means 3a will transmit the user registration number 9b and the multimedia information number 10b to the control means 8d. The control means 8d picks out a user's contract information record 9a by making the user registration number 9b into a search condition from the user information data base 9a and outputs the contract type 9e to the execution information transmission system determination means 8f. The execution information transmission system determination means 8f has a list of number of an execution information transmission system which can be used by the execution information control means 3a in an inside and outputs a system number of a system which chose and chose one in a list from the contract type 9e to the control means 8d. The control means 8d transmits a system number to the execution information control means 3a. The execution information control means 3a will transmit execution information to the control means 8d based on an execution information transmission system of a system number if a system number is received.

[0061]The transmission system of execution information has a system system which transmits execution information a system which transmits execution information with a certain fixed time interval or a system which transmits execution information with an irregular time interval only when a user's demand is during information execution.

[0062]As mentioned above since a user and a third party intercept at time to send execution information by changing the system which transmits execution information to a multimedia information server and it becomes impossible to transmit the execution information of ** according to this embodiment it is effective in preventing execution of unjust multimedia information.

[0063]As opposed to the user information data base which embodiment 10. drawing 18 is a block diagram of the user information data base in Embodiment 10 and was shown in drawing 2. The multimedia information numbers 9f and 9h and the multimedia execution control information 9g and 9i are added and the number and execution control information on multimedia information that the user has made a contract of service are held. The system configuration of this embodiment is the same as that of what was shown in drawing 14.

[0064]Next operation is explained. If a user chooses one multimedia information the execution information control means 3a will transmit the user registration number 9b and the multimedia information number 10b to the control means 8d. The control means 8d picks out a user's contract information record 9a by making the user registration number 9b into a search condition from the user information data base 9a and checks whether the multimedia information number 10b which the user is

demanding of the multimedia information numbers 9f and 9h in it is included. The control means 8d will judge whether the start of execution of multimedia information is possible based on the multimedia execution control information 9g and 9i corresponding to the multimedia information numbers 9f and 9h if the number which the user is demanding is found. When there is no number which the user is demanding it is judged whether the start of execution is possible at the time which had [whether multimedia information with a demand can be performed based on the contract type 9e and] the demand again.

[0065] If a user's control request occurs during execution of multimedia information the execution information control means 3a will transmit to the control means 8d by making the demand into execution information. It is judged whether based on the multimedia execution control information 9g and 9i this demand can perform the control means 8d. If judged with it being possible the message which can be performed to the execution information control means 3a will be transmitted. The execution information control means 3a controls the execution means 3b based on a user's demand. If judged with it being impossible a message [that it cannot perform to the execution information control means 3a] will be transmitted. The execution information control means 3a outputs a canceling [a user's demand] **** message to the input/output device 1.

[0066] As mentioned above according to this embodiment the execution control information on the multimedia information which the user has made a contract of is stored in a user information data base. Since it distinguishes whether multimedia information is performed based on this execution control information and transmission of multimedia information is controlled it is effective in preventing execution of the unjust multimedia information which breaks conditions of contract.

[0067] Embodiment 11. drawing 19 is a block diagram of the multimedia information database in Embodiment 11 and has added the execution constraints 10e which restrain execution of multimedia information to the multimedia information database shown in drawing 3. The system configuration of this embodiment is the same as that of what was shown in drawing 14.

[0068] Next operation is explained. If a user chooses one multimedia information the execution information control means 3a will transmit the user registration number 9b and the multimedia information number 10b to the control means 8d. The control means 8d picks out the contract type 9e of a user in a user's contract information record 9a from the user information data base 9 by making the user registration number 9b into a search condition. The control means 8d takes out the execution constraints 10e in the multimedia information record 10a from the multimedia information database 10 by making the multimedia information number 10b into a search condition and checks whether a user's contract type 9e is included in the execution constraints 10e. When contained it is judged whether a start of execution is possible at time which a demand suited [whether multimedia information with a

demand can be performed from the contract type 9eand] again. When not contained a message which shows that a demand from a user was canceled and a demand from a user was canceled is transmitted to the execution information control means 3a. The execution information control means 3a outputs a canceling [a user's demand] **** message to the input/output device 1.

[0069]As mentioned aboveaccording to this embodimentexecution constraints for performing multimedia information are stored in a multimedia information databaseSince it distinguishes whether multimedia information is performed based on these execution constraints and transmission of multimedia information is controlledit is effective in preventing execution of unjust multimedia information which breaks conditions of contract.

[0070]

[Effect of the Invention]As mentioned abovethe encoding means which enciphers the invention ***** according to claim 1 and multimedia informationSince the cipher system is changed for every user by determining the decoding means which decodes the multimedia information enciphered by this encoding means based on contract information with a userSince the guess of a cipher system is difficult for a third partyit is effective in the ability to eliminate unjust access to multimedia information.

[0071]By according to the invention according to claim 2having a cipher system memory measure which memorizes two or more encoding means and two or more decoding meansand determining an encoding means and a decoding means based on contract information with a userSince the cipher system is changed for every userand the guess of a cipher system is difficult for a third partyit is effective in the ability to eliminate unjust access to multimedia information.

[0072]According to the invention according to claim 3the transmitting means which transmits encryption multimedia informationThe reception means which is provided with the cipher system memory measure which memorizes two or more encoding meansand decodes encryption multimedia informationSince it had the decode system memory measure which memorizes two or more decoding meansin order that there may be no necessity of transmitting a decoding means to a client from a serverit is effective in the ability to shorten a part for the air time of a decoding means.

[0073]Since according to the invention according to claim 4 it has an area information memory measure which memorizes the area information which shows the usable area of an encoding means and an encoding means and a decoding means are determined based on contract information and area information with a userAlso when the cipher system which can be used changes with areasit is effective in the ability to choose a cipher system.

[0074]According to the invention according to claim 5the transmitting means of a serverEquip the encryption execution means which is not under execution with the cipher system alteration means which performs encryptionand the reception means of a clientSince the cipher system used by having equipped the decoding execution

means which is not under execution with the decode system alteration means which performs decoding can be changed dynamically when adding a cipher system it is effective in that there is no necessity of changing the hardware which constitutes a system.

[0075] According to the invention according to claim 6 since a cipher system can be known from send data by storing the classification of the encoding means used into the send data of encryption multimedia information there is no necessity of notifying a cipher system to a client and it is effective in the ability to shorten time.

[0076] Since it distinguishes whether the execution information which shows the run state of the multimedia information in a client side is compared with contract information with a user and multimedia information is performed based on a contract according to the invention according to claim 7 it is effective in preventing execution of the unjust multimedia information which breaks conditions of contract.

[0077] Since it intercepts at time to send execution information by determining the execution information transmission system from a client to a server based on contract information with a user and it becomes impossible to transmit the execution information of ** according to the invention according to claim 8 it is effective in preventing execution of the unjust multimedia information which breaks conditions of contract.

[0078] According to the invention according to claim 9 the execution control information on the multimedia information which the user has made a contract of is stored in the User Information memory measure. Since it distinguishes whether multimedia information is performed based on this execution control information and transmission of multimedia information is controlled it is effective in preventing execution of the unjust multimedia information which breaks conditions of contract.

[0079] According to the invention according to claim 10 the execution constraints which restrain execution of multimedia information are stored in a multimedia information memory measure. Since it distinguishes whether multimedia information is performed based on these execution constraints and transmission of multimedia information is controlled it is effective in preventing execution of the unjust multimedia information which breaks conditions of contract.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is a block diagram of the multimedia information system of Embodiment 1.

[Drawing 2] It is a block diagram of a user information data base.

[Drawing 3] It is a block diagram of a multimedia information database.

[Drawing 4] It is a block diagram of a cipher system database.

[Drawing 5] It is a flow chart which shows operation of the multimedia information system of Embodiment 1.

[Drawing 6] It is a block diagram of the multimedia information system of Embodiment 2.

[Drawing 7] It is a block diagram of the multimedia information system of Embodiment 3.

[Drawing 8] It is a block diagram of the multimedia information system of Embodiment 4.

[Drawing 9] It is a block diagram of the cipher system database of Embodiment 5.

[Drawing 10] It is a block diagram of the multimedia information system of Embodiment 6.

[Drawing 11] It is a flow chart which shows operation of the multimedia information system of Embodiment 6.

[Drawing 12] It is a flow chart which shows the operation in the case of changing the cipher system in the multimedia information system of Embodiment 6.

[Drawing 13] It is a block diagram of the send data of the multimedia information server in Embodiment 7.

[Drawing 14] It is a block diagram of the multimedia information system of Embodiment 8.

[Drawing 15] It is a flow chart which shows operation of the multimedia information system of Embodiment 8.

[Drawing 16] It is a flow chart which shows the operation under multimedia information execution in the multimedia information system of Embodiment 8.

[Drawing 17] It is a block diagram of the multimedia information system of Embodiment 9.

[Drawing 18] It is a block diagram of the user information data base in Embodiment 10.

[Drawing 19] It is a block diagram of the multimedia information database in Embodiment 11.

[Drawing 20] It is an outline block diagram of the conventional multimedia information system.

[Drawing 21] It is a block diagram of the media data in the conventional multimedia information system.

[Explanations of letters or numerals]

1 A multimedia client and 2 An input output means and 3 Execution control means 3a An execution information control means and 3b An execution means and 4 A reception means and 4a Decode system alteration means 4b and 4c A decoding execution means and 4 d A reception control means and 5 Network 6 multimedia-information server and 7 A transmitting means and 7a Cipher system alteration means 7b and 7c An encryption execution means and 7 d A transmission control means and 8 Information control means 8a A ciphering system deciding means and 8b A cipher system transmitting means and 8c Key generation part 8 d A control

means8e multimedia information transmitting meansand 8 f Execution information transmission system determination means9 A user information data base and 9a A contract information record9b user registration number9c A name and 9 d An address9e contract type9f multimedia information number9 g Multimedia execution control information9h multimedia information number9i multimedia execution control information10 multimedia-information database10a The name of a multimedia information record10b multimedia information numberand 10c multimedia informationand 10 d A real whereabouts type number and 10e Execution constraints10f multimedia information11 cipher-system databaseand 11a Cipher system record11b cipher system number and 11c The name of a cipher systemand 11 d Key generating means11e An encoding means and 11 f [A decoding means database and 13 / An encoding means database14 send dataand 14a / A cipher system number and 14b / Real whereabouts type database.] The multimedia information and 15 which were enciphered A decoding means and 11 g Usable area information and 12

特開平10-177523

(43) 公開日 平成10年(1998) 6月30日

(51) Int.Cl. ⁴	識別記号	F I
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14 3 2 0 B
12/00	5 3 7	12/00 5 3 7 H
	5 4 7	5 4 7 D
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00 6 6 0 D
H 0 4 L 9/14		H 0 4 L 9/00 6 4 1
審査請求 未請求 請求項の数10 O.L. (全 18 頁)		

審査請求 未請求 請求項の数10 O L (全 18 頁)

(21) 出願番号 特願平8-335594

(22) 出願日 平成8年(1996)12月16日

(71) 出願人 000008013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 藤井 誠司

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

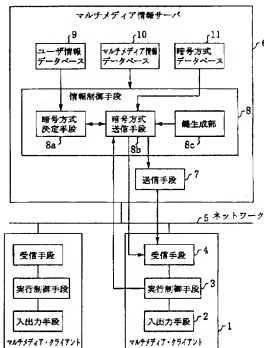
(74) 代理人 弁理士 宮田 金雄 (外2名)

(54) 【発明の名称】 マルチメディア情報システム

(57) 【要約】

【課題】 マルチメディア情報への不正なアクセスを排除し、ユーザが契約条件に基づいてマルチメディア情報を実行することを保証する。

【解決手段】 マルチメディア情報サーバ6は、マルチメディア情報を暗号化する暗号化手段と暗号化マルチメディア情報を復号する復号手段とをユーザ情報データベース9に記憶されたユーザとの契約情報に基づいて決定する暗号方式決定手段8aと、この暗号方式決定手段8aにより決定された暗号化手段を用いて、マルチメディア情報データベース10に記憶されたマルチメディア情報を暗号化し、この暗号化マルチメディア情報を送信する送信手段7とを備え、マルチメディア・クライアント1は、暗号方式決定手段8aにより決定された復号手段を用いて、送信手段7により送信された暗号化マルチメディア情報を復号する受信手段4を備えた。



【特許請求の範囲】

【請求項 1】 以下の要素を備えたマルチメディア情報システム。

(a) ユーザとの契約情報を記憶するユーザ情報記憶手段；

(b) 文字、図形、音声、静止画又は動画を含むマルチメディア情報を記憶するマルチメディア情報記憶手段；

(c) 以下の要素を備えたサーバ；

(c 1) 上記マルチメディア情報を暗号化する暗号化手段と、この暗号化手段により暗号化されたマルチメディア情報を復号する復号手段とを、上記ユーザ情報記憶手段に記憶された上記契約情報に基づいて決定する暗号方式決定手段；

(c 2) この暗号方式決定手段により決定された暗号化手段を用いて、上記マルチメディア情報記憶手段に記憶されたマルチメディア情報を暗号化し、この暗号化されたマルチメディア情報を送信する送信手段；

(d) 以下の要素を備え、上記サーバに上記マルチメディア情報の送信を要求するクライアント；

(d 1) 上記暗号方式決定手段により決定された復号手段を用いて、上記送信手段により送信された暗号化マルチメディア情報を復号する受信手段。

【請求項 2】 それぞれ異なる暗号化を行なう複数の暗号化手段とこの各暗号化手段により暗号化されたデータを復号する複数の復号手段とを記憶する暗号方式記憶手段を備え、

上記サーバは、上記暗号方式決定手段により決定された暗号化手段と復号手段とを上記暗号方式記憶手段より取り出し、この取り出した暗号化手段と復号手段とを送信する暗号方式送信手段を備え、

上記送信手段は、上記暗号方式送信手段により送信された暗号化手段を用いて暗号化し、

上記受信手段は、上記暗号方式送信手段により送信された復号手段を用いて復号することを特徴とする請求項 1 記載のマルチメディア情報システム。

【請求項 3】 上記送信手段は、それぞれ異なる暗号化を行なう複数の暗号化手段を記憶する暗号方式記憶手段を備え、上記暗号方式決定手段より取り出した暗号化手段を上記暗号方式記憶手段より取り出し、この取り出した暗号化手段を用いて暗号化し、

上記受信手段は、上記暗号方式記憶手段に記憶された暗号化手段により暗号化されたデータを復号する複数の復号手段を記憶する復号方式記憶手段を備え、上記暗号方式決定手段により決定された復号手段を上記復号方式記憶手段より取り出し、この取り出した復号手段を用いて復号することを特徴とする請求項 1 記載のマルチメディア情報システム。

【請求項 4】 上記暗号化手段の使用可能な地域を示す地域情報を記憶する地域情報記憶手段を備え、上記暗号方式決定手段は、上記ユーザ情報記憶手段に記

憶された上記契約情報と上記地域情報記憶手段に記憶された上記地域情報とに基づいて、上記暗号化手段と上記復号手段とを決定することを特徴とする請求項 1 記載のマルチメディア情報システム。

【請求項 5】 上記暗号方式決定手段は、新たに決定した暗号化手段と復号手段とを送信し、

上記送信手段は、

上記マルチメディア情報記憶手段に記憶されたマルチメディア情報を暗号化する暗号化手段を実行する複数の暗号化実行手段と、

上記暗号方式決定手段により送信された新たな暗号化手段を、実行中でない上記暗号化実行手段に実行させる暗号方式変更手段と、

上記暗号化実行手段により暗号化されたマルチメディア情報を送信する送信制御手段とを備え、

上記受信手段は、

上記送信制御手段により送信された暗号化マルチメディア情報を復号する復号手段を実行する複数の復号実行手段と、

上記暗号方式決定手段により送信された新たな復号手段を、実行中でない上記復号実行手段に実行させる復号方式変更手段とを備えたことを特徴とする請求項 1 記載のマルチメディア情報システム。

【請求項 6】 上記送信制御手段は、上記暗号化実行手段により暗号化されたマルチメディア情報と暗号化するために使用した暗号化手段の種別とを格納した送信データを構築して送信し、

上記復号方式変更手段は、上記送信データを受信し、この受信したデータに格納された上記種別に基づいて上記マルチメディア情報を暗号化した暗号化手段を判別し、この暗号化手段に対応した復号手段を上記復号実行手段に実行させることを特徴とする請求項 5 記載のマルチメディア情報システム。

【請求項 7】 以下の要素を備えたマルチメディア情報システム。

(a) ユーザとの契約情報を記憶するユーザ情報記憶手段；

(b) 文字、図形、音声、静止画又は動画を含むマルチメディア情報を記憶するマルチメディア情報記憶手段；

(c) 以下の要素を備えたサーバ；

(c 1) 上記マルチメディア情報記憶手段に記憶されたマルチメディア情報を暗号化し、この暗号化されたマルチメディア情報を送信する送信手段；

(c 2) 上記マルチメディア情報の実行情報を受信し、この実行情報と上記ユーザ情報記憶手段に記憶された契約情報とを照合し、上記契約情報に基づいて上記マルチメディア情報を実行しているか否かを判別し、上記送信手段によるマルチメディア情報の送信を制御する制御手段；

(d) 以下の要素を備え、上記サーバに上記マルチメデ

ィア情報の送信を要求するクライアント；

(d1) 上記送信手段により送信された暗号化マルチメディア情報を復号する受信手段；

(d2) この受信手段により復号されたマルチメディア情報を実行する実行手段；

(d3) この実行手段の実行中の状態を示す実行情報を上記制御手段に送信する実行情報送信手段。

【請求項8】 上記サーバは、上記実行情報送信手段による上記実行情報の送信方式を上記ユーザ情報記憶手段に記憶された契約情報に基づいて決定する実行情報送信方式決定手段を備え、

上記実行情報送信手段は、上記実行情報送信方式決定手段により決定された送信方式により上記実行情報を送信することを特徴とする請求項7記載のマルチメディア情報システム。

【請求項9】 上記ユーザ情報記憶手段は、ユーザとの契約情報と、マルチメディア情報に対する実行制御情報とを記憶し、

上記制御手段は、上記受信した実行情報を上記ユーザ情報記憶手段に記憶された契約情報及び実行制御情報と照合し、上記契約情報及び上記実行制御情報に基づいて上記マルチメディア情報を実行しているか否かを判別し、上記マルチメディア情報の送信を制御することを特徴とする請求項7記載のマルチメディア情報システム。

【請求項10】 上記マルチメディア情報記憶手段は、上記マルチメディア情報とこのマルチメディア情報の実行を制約する実行制約条件とを記憶し、

上記制御手段は、上記受信した実行情報を、上記ユーザ情報記憶手段に記憶された契約情報、及び、上記マルチメディア情報記憶手段に記憶された実行制約条件と照合し、上記契約情報及び上記実行制約条件に基づいて上記マルチメディア情報を実行しているか否かを判別し、上記マルチメディア情報の送信を制御することを特徴とする請求項7記載のマルチメディア情報システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、契約したユーザに文字、図形、音声、静止画又は動画からなるマルチメディア情報を暗号化して提供するマルチメディア情報システムに関するものである。

【0002】

【従来の技術】 図20は、例えば特開平6-44122号公報に示された従来のマルチメディア情報システムを示す概略構成図である。図において、50は文字、図形、音声、静止画、動画などの各種メディアデータからなるマルチメディアファイルの暗号化して蓄積するマルチメディア情報蓄積部、51はマルチメディア情報蓄積部50に対するマルチメディアファイルの入出力を管理するマルチメディア情報管理部、52はマルチメディアファイルの内容を表示する出力装置である。

【0003】 図21はマルチメディア情報蓄積部50に蓄積されるマルチメディアファイルの構成要素であるメディアデータの構成図である。図において、60はメディアデータ、60aはユーザのセキュリティレベルに応じてアクセス可能なデータが否かを判別するための暗号化鍵情報、60bはディスプレイ画面上での表示位置や表示する大きさを示す位置・大きさ情報、60cはメディアデータのメディア種別を示すメディア種類情報、60dは提示能力の異なるディスプレイ画面への対応のために入力時とは別のデータ形式のデータを付加した出力装置対応データである。このように、ユーザによるアクセスが可能か否かを判別するための暗号化鍵情報をメディアデータ毎に有しており、マルチメディアファイルを構成している一つ一つのメディアデータ単位でセキュリティレベルを変えることができる。

【0004】 次に動作について説明する。ユーザがマルチメディアファイルの出力をマルチメディア情報管理部51に要求すると、マルチメディア情報管理部51は、出力要求のあったマルチメディアファイルを構成しているメディアデータ60をマルチメディア情報蓄積部50から取り出す。次に、マルチメディア情報管理部51は、ユーザのセキュリティレベルを解析し、各メディアデータ60に含まれる暗号化鍵情報60aに基づき、そのユーザのセキュリティレベルでアクセス可能なメディアデータであるか否かを判別する。そして、ユーザがアクセス可能なメディアデータであると判別した時、このアクセス可能なメディアデータ60のみを出力の対象とし、出力装置52の提示能力に応じたデータ形式に変換して、出力装置52へ出力する。

【0005】

【発明が解決しようとする課題】 従来のマルチメディア情報システムは、以上のように構成されており、暗号化したマルチメディア情報を蓄積し、ユーザへ送信している。そのため、長期間に渡って同じ暗号方式を使用することになり、契約しているユーザ以外の第三者によって通信データが盗聴され暗号方式を解読されるので、ユーザに送信しているマルチメディア情報へ第三者が不正にアクセスできるという問題点があった。

【0006】 また、ユーザのマルチメディア情報の実行に関する契約条件をマルチメディア情報を送信の前に確認するだけであり、マルチメディア情報の実行中は、ユーザが契約条件に基づいて正しく実行しているか否かチェックできないため、マルチメディア情報不正に実行できてしまうという問題点があった。

【0007】 また、日、時、時間帯単位によるマルチメディア情報の実行、実行回数などの様々なユーザのマルチメディア情報の実行に関する契約条件に応じたマルチメディア情報の実行を制御することができないという問題点があった。

【0008】 この発明は、上記のような問題点を解消す

るためになされたものであり、第三者によるマルチメディア情報への不正なアクセスを排除し、ユーザが契約条件に基づいてマルチメディア情報を実行することを保証するマルチメディア情報システムを得ることを目的とする。

【0009】

【課題を解決するための手段】請求項1記載のマルチメディア情報システムは、以下の要素を備えたものである。

(a) ユーザとの契約情報を記憶するユーザ情報記憶手段；

(b) 文字、図形、音声、静止画又は動画を含むマルチメディア情報を記憶するマルチメディア情報記憶手段；

(c) 以下の要素を備えたサーバ；

(c1) 上記マルチメディア情報を暗号化する暗号化手段と、この暗号化手段により暗号化されたマルチメディア情報を復号する復号手段とを、上記ユーザ情報記憶手段に記憶された上記契約情報に基づいて決定する暗号方式決定手段；

(c2) この暗号方式決定手段により決定された暗号化手段を用いて、上記マルチメディア情報記憶手段に記憶されたマルチメディア情報を暗号化し、この暗号化したマルチメディア情報を送信する送信手段；

(d) 以下の要素を備え、上記サーバに上記マルチメディア情報の送信を要求するクライアント；

(d1) 上記暗号方式決定手段により決定された復号手段を用いて、上記送信手段により送信された暗号化マルチメディア情報を復号する受信手段。

【0010】請求項2記載のマルチメディア情報システムは、それぞれ異なる暗号化を行なう複数の暗号化手段とこの各暗号化手段により暗号化されたデータを復号する複数の復号手段とを記憶する暗号方式記憶手段を備え、上記サーバは、上記暗号方式決定手段により決定された暗号化手段と復号手段とを上記暗号方式記憶手段より取り出し、この取り出した暗号化手段と復号手段とを送信する暗号方式送信手段を備え、上記送信手段は、上記暗号方式送信手段により送信された暗号化手段を上記暗号方式記憶手段を用いて暗号化し、上記受信手段は、上記暗号方式送信手段により送信された復号手段を用いて復号するものである。

【0011】請求項3記載のマルチメディア情報システムは、それぞれ異なる暗号化を行なう複数の暗号化手段を記憶する暗号方式記憶手段を有し、上記暗号方式決定手段により決定された暗号化手段を上記暗号方式記憶手段より取り出し、この取り出した暗号化手段を用いて暗号化する送信手段と、上記暗号方式記憶手段に記憶された暗号化手段により暗号化されたデータを復号する複数の復号手段を記憶する復号方式記憶手段を有し、上記暗号方式決定手段により決定された復号手段を上記復号方式記憶手段より取り出し、この取り出した復号手段を用いて復号する受信手段とを備えたものである。

【0012】請求項4記載のマルチメディア情報システムは、上記暗号化手段の使用可能な地域を示す地域情報を記憶する地域情報記憶手段を備え、上記暗号方式決定手段は、上記ユーザ情報記憶手段に記憶された上記契約情報と上記地域情報記憶手段に記憶された上記地域情報とに基づいて、上記暗号化手段と上記復号手段とを決定するものである。

【0013】請求項5記載のマルチメディア情報システムは、新たに決定した暗号化手段と復号手段とを送信する暗号方式決定手段を備え、上記送信手段は、上記マルチメディア情報記憶手段に記憶されたマルチメディア情報を暗号化する暗号化手段を実行する複数の暗号化実行手段と、上記暗号方式決定手段により送信された新たな暗号化手段を、実行中でない上記暗号化実行手段に実行させる暗号方式変更手段と、上記暗号化実行手段により暗号化されたマルチメディア情報を送信する送信制御手段とを備え、上記受信手段は、上記送信制御手段により送信された暗号化マルチメディア情報を復号する復号手段を実行する複数の復号実行手段と、上記暗号方式決定手段により送信された新たな復号手段を、実行中でない上記復号実行手段に実行させる復号方式変更手段とを備えたものである。

【0014】請求項6記載のマルチメディア情報システムは、上記暗号化実行手段により暗号化されたマルチメディア情報と暗号化するために使用した暗号化手段の種別とを格納した送信データを構築して送信する送信制御手段と、上記送信データを受信し、この受信したデータに格納された上記種別に基づいて上記マルチメディア情報を暗号化した暗号化手段を判別し、この暗号化手段に対応した復号手段を上記復号実行手段に実行させる復号方式変更手段とを備えたものである。

【0015】請求項7記載のマルチメディア情報システムは、以下の要素を備えたものである。

(a) ユーザとの契約情報を記憶するユーザ情報記憶手段；

(b) 文字、図形、音声、静止画又は動画を含むマルチメディア情報を記憶するマルチメディア情報記憶手段；

(c) 以下の要素を備えたサーバ；

(c1) 上記マルチメディア情報記憶手段に記憶されたマルチメディア情報を暗号化し、この暗号化したマルチメディア情報を送信する送信手段；

(c2) 上記マルチメディア情報の実行情報を受信し、この実行情報と上記ユーザ情報記憶手段に記憶された契約情報とを照合し、上記契約情報に基づいて上記マルチメディア情報を実行しているか否かを判別し、上記送信手段によるマルチメディア情報の送信を制御する制御手段；

(d) 以下の要素を備え、上記サーバに上記マルチメディア情報の送信を要求するクライアント；

(d1) 上記送信手段により送信された暗号化マルチメ

ディア情報を復号する受信手段；

(d2) この受信手段により復号されたマルチメディア情報を実行する実行手段；

(d3) この実行手段の実行中の状態を示す実行情報を上記制御手段に送信する実行情報送信手段。

【0016】請求項8記載のマルチメディア情報システムは、上記実行情報送信手段による上記実行情報の送信方式を上記ユーザ情報記憶手段に記憶された契約情報に基づいて決定する実行情報送信方式決定手段を上記サーバに備え、上記実行情報送信手段は、上記実行情報送信方式決定手段により決定された送信方式により上記実行情報を送信するものである。

【0017】請求項9記載のマルチメディア情報システムは、ユーザとの契約情報と、マルチメディア情報に対する実行制御情報とを記憶するユーザ情報記憶手段と、上記受信した実行情報を上記ユーザ情報記憶手段に記憶された契約情報及び実行制御情報と照合し、上記契約情報及び上記実行制御情報に基づいて上記マルチメディア情報を実行しているか否かを判別し、上記マルチメディア情報の送信を制御する制御手段とを備えたものである。

【0018】請求項10記載のマルチメディア情報システムは、上記マルチメディア情報とこのマルチメディア情報の実行を制約する実行制約条件とを記憶するマルチメディア情報記憶手段と、上記受信した実行情報を、上記ユーザ情報記憶手段に記憶された契約情報、及び、上記マルチメディア情報記憶手段に記憶された実行制約条件と照合し、上記契約情報及び上記実行制約条件に基づいて上記マルチメディア情報を実行しているか否かを判別し、上記マルチメディア情報の送信を制御する制御手段とを備えたものである。

【0019】

【発明の実施の形態】

実施の形態1。以下、本発明を実施の形態に基づいて、図を参照しながら、説明する。図1は、実施の形態1のマルチメディア情報システムの構成図である。図において、1はマルチメディア情報の送信を要求するマルチメディア・クライアント、2はユーザからの要求を受け付けるとともに、マルチメディア情報の実行結果を出力する入出力手段、3はマルチメディア情報を実行し、実行結果を入出力手段2に送信する実行制御手段、4は暗号化されたマルチメディア情報を受信して復号し、実行制御手段3に送信する受信手段、5はネットワーク、6はマルチメディア情報サーバ、7はマルチメディア情報を暗号化し、マルチメディア・クライアント1へネットワーク5を経由して送信する送信手段、8は暗号方式を決定するとともに、マルチメディア情報の送信を制御する情報制御手段、9は契約しているすべてのユーザの契約情報を蓄積しているユーザ情報記憶手段としてのユーザ情報データベース、10はマルチメディア情報サーバ6

がサービスを提供するすべてのマルチメディア情報を蓄積しているマルチメディア情報記憶手段としてのマルチメディア情報データベース、11はマルチメディア情報サーバ6で使用できるすべての暗号方式の鍵生成手段、暗号化手段及び復号手段を蓄積している暗号方式記憶手段としての暗号方式データベースである。

【0020】情報制御手段8は、暗号方式決定手段8a、暗号方式送信手段8b、鍵生成部8cから構成されている。暗号方式決定手段8aは、ユーザ情報データベース9に蓄積されているユーザの契約情報に基づいてマルチメディア情報を送信する時に使用する暗号方式を決定する。暗号方式送信手段8bは、暗号方式決定手段8aにより決定された暗号方式の鍵生成手段、暗号化手段及び復号手段を暗号方式データベース11から取り出し、鍵生成手段は鍵生成部8cへ、暗号化手段は送信手段7へ、復号手段は受信手段4へ送信する。鍵生成部8cは、暗号方式送信手段8bにより送信された鍵生成手段を用いて、暗号化鍵と復号鍵を生成する。

【0021】本システムは、図示したように、マルチメディア情報サーバ6と、複数のマルチメディア・クライアント1とが、ネットワーク5に接続されており、マルチメディア情報サーバ6は、マルチメディア・クライアント1から要求されたマルチメディア情報をマルチメディア情報データベース10より取り出して暗号化し、マルチメディア・クライアント1に送信するものである。

【0022】図2は、ユーザ情報データベース10に蓄積されている契約情報の構成を示す構成図である。図において、9aはユーザとの契約情報記録、9bはユーザ登録番号、9cはユーザの氏名、9dはユーザの住所、9eはユーザとの契約タイプである。契約タイプ9eは暗号方式を決定するための情報である。

【0023】図3は、マルチメディア情報データベース10に蓄積されているマルチメディア情報の構成を示す構成図である。図において、10aはマルチメディア情報記録、10bはマルチメディア情報を一意に識別するためのマルチメディア情報番号、10cはマルチメディア情報の名称、10dはマルチメディア情報の実行手段を示す実行方式番号、10fはマルチメディア情報である。

【0024】図4は、暗号方式データベース11に蓄積されている暗号方式の構成を示す構成図である。図において、11aは暗号方式記録、11bは暗号方式を一意に識別するための暗号方式番号、11cは暗号方式の名称、11dは暗号化鍵と復号鍵を生成する鍵生成手段、11eはマルチメディア情報を暗号化する暗号化手段、11fは暗号化されたマルチメディア情報を復号する復号手段である。

【0025】次に動作について、図5のフローチャートに基づいて説明する。入出力手段2に表示されているマルチメディア情報番号10aとマルチメディア情報名称1

0 cの中から、ユーザが一つのマルチメディア情報番号10 aを選択すると(ステップS1)、実行制御手段3は、ユーザにより入力されたユーザ登録番号9 bと、選択されたマルチメディア情報番号10 aとを、マルチメディア情報サーバ6の暗号方式送信手段8 bへ送信する(ステップS2)。暗号方式送信手段8 bは、ユーザ登録番号9 bを暗号方式決定手段8 aへ出力する(ステップS3)。

【0026】暗号方式決定手段8 aは、ユーザ登録番号9 bを検索条件としてユーザ情報データベース9からユーザの契約情報レコード9 aを取得し(ステップS4)、取得した契約情報レコード9 a中の契約タイプ9 eに基づいて暗号方式を決定し、決定した暗号方式の暗号方式番号11 bを暗号方式送信手段8 bへ出力する(ステップS5)。

【0027】暗号方式送信手段8 bは、暗号方式番号11 bを検索条件として、暗号方式データベース11から鍵生成手段11 d、暗号化手段11 e及び復号手段11 fを取得する(ステップS6)。暗号方式送信手段8 bは、鍵生成手段11 dを鍵生成部8 cへ出力し(ステップS7)、鍵生成部8 cは、この出力された鍵生成手段11 dを使用して、暗号化鍵と復号鍵を生成し、暗号方式送信手段8 bへ出力する(ステップS8)。暗号方式送信手段8 bは、鍵生成部8 cにより生成された暗号化鍵と、暗号方式データベース11から取得した暗号化手段11 eとを送信手段7へ出力し(ステップS9)、鍵生成部8 cにより生成された復号鍵と、暗号方式データベース11から取得した復号手段11 fを受信手段4へ送信する(ステップS10)。

【0028】そして次に、暗号方式送信手段8 bは、ステップS2で送信されたマルチメディア情報番号10 aを検索条件として、ユーザが選択したマルチメディア情報10 fをマルチメディア情報データベース10から取り出し、ブロックに分割して送信手段7へ出力する(ステップS11)。送信手段7は、ステップS9で出力された暗号化鍵と暗号化手段11 eを用いて、マルチメディア情報10 fの各ブロックを暗号化し、受信手段4へ送信する(ステップS12)。

【0029】受信手段4は、受信した暗号化マルチメディア情報10 fの各ブロックを、ステップS10で送信された復号鍵と復号手段11 fとを用いて復号し、実行制御手段3へ送信する(ステップS13)。実行制御手段3は、復号されたマルチメディア情報10 fを実行し、実行結果を出力手段2へ出力する(ステップS14)。

【0030】以上のように、この実施の形態によれば、暗号方式データベース11に蓄積されている多数の暗号方式の中から、ユーザの契約タイプに基づいて暗号方式を選択し、ユーザ毎に暗号方式を変更しているため、第三者は暗号方式の推測が困難であるため、不正なアクセ

スが排除できるという効果がある。

【0031】なお、この実施の形態では、暗号方式決定手段8 aが暗号方式を決定し、暗号方式送信手段8 bが鍵生成手段、暗号化手段及び復号手段を送信する形態を示したが、暗号方式決定手段8 aが暗号方式送信手段8 bの機能を有し、決定した暗号方式に対応する各手段を送信するように構成することも出来る。

【0032】実施の形態2。送信手段7で実行する暗号化手段や、受信手段4で実行する復号手段が変更できない場合には、図6に示すように、複数の異なる暗号方式の送信手段7と受信手段4とを用いて、情報制御手段8が送信手段7を切り替え、実行制御手段3へ同じ暗号方式の受信手段4を使用するように命令して切り替えることにより、マルチメディア情報システムを実現することもできる。

【0033】実施の形態3。また、ネットワークを経由して復号手段11 fを送信する場合、第三者に復号手段11 fを盗まれる可能性があることや、復号手段11 fを受信手段4へ送信する時間を短縮するため、図7に示すように、マルチメディア・クライアント側に復号手段だけを蓄積した復号手段データベース12を分散して配置することもできる。

【0034】実施の形態4。さらに、図8に示すように、マルチメディア情報サーバ側の送信手段7が暗号化手段データベース13を持ち、マルチメディア・クライアント側の受信手段4が復号手段データベース12を内部に持つように構成することもできる。

【0035】実施の形態5。実施の形態1では、ユーザとの契約情報中の契約タイプに基づいて暗号方式を決定したが、契約タイプに合致する暗号方式の候補が複数残った場合に暗号方式を1つに決定するためには、契約タイプ以外の情報が必要になる。

【0036】ユーザとマルチメディア情報サーバとの間で暗号化したデータを送受信するとき、使用可能な暗号方式が居住地域の法律によって制限されることがある。マルチメディア・クライアントが存在する地域で使用可能な暗号方式と、マルチメディア情報サーバが存在する地域で使用可能な暗号方式とで、まったく同じ暗号方式が使用できるとは限らないので、両方の場所で使用できる暗号方式を決定する必要があるが、これはユーザ個人との契約条件だけでは判断できない。そこで、この実施の形態では、暗号方式データベースを図9に示す構造にする。図9に示した暗号方式データベースは、図4に示した暗号方式データベースに対して、各暗号方式の使用可能地域を示す使用可能地域情報11 gを追加したものである。

【0037】この実施の形態のマルチメディア情報システムの構成は、実施の形態1で説明した図1の構成と同様であるが、暗号方式決定手段8 aにおける暗号方式決定の動作が実施の形態1のものと異なる。異なる動作

は、実施の形態1で説明したステップS4、S5である。異なる動作を次に説明する。この実施の形態では、暗号方式決定手段8aは、ユーザ登録番号9bを検索条件としてユーザ情報データベース9からユーザの契約情報レコード9aを取得する。次に、図8に示した暗号方式データベース11から暗号方式レコード11aを取り出す。そして、取得した契約情報レコード9a中の住所9dが、暗号方式レコード11a中の使用可能地域情報11gに合致するかどうかを調べる。合致する暗号方式が複数である場合は、その中からユーザの契約情報レコード9a中の契約タイプ9eに合致する暗号方式を決定し、決定した暗号方式の暗号方式番号11bを暗号方式送信手段8bへ出力する。

【0038】以上のように、この実施の形態によれば、ユーザの契約タイプと、暗号方式の使用可能地域情報とに基づいて暗号方式を決定するで、使用できる暗号方式が地域によって異なる場合にも、暗号方式を選択することができ。

【0039】実施の形態6、図10は、実施の形態6のマルチメディア情報システムの構成図である。図において、実行制御手段3と受信手段4は、図1に示したものと同様マルチメディア・クライアントを構成し、送信手段7と情報制御手段8は、図1に示したものと同様マルチメディア情報サーバを構成する。

【0040】情報制御手段8において、暗号方式決定手段8aは、暗号方式が変更になったときは、新たに暗号方式を決定し、暗号方式送信手段8bは、新たな暗号方式に基づいて、鍵生成手段、暗号化手段及び復号手段を図1に示した暗号方式データベース11から取り出し、鍵生成手段は鍵生成部8cへ、暗号化手段は送信手段7へ、復号手段は受信手段4へ送信する。送信手段7は、暗号方式変更手段7a、暗号化実行手段7b、7c及び送信制御手段7dから構成されている。暗号方式変更手段7aは、暗号方式送信手段8bにより送信された新たな暗号化手段に基づいて、送信手段7で使用する暗号化実行手段7b、7cを切り替える。暗号化実行手段7b、7cは、暗号方式送信手段8bから送信された暗号化手段を実行するものであり、送信制御手段7dから出力されるデータを暗号化し、その結果を送信制御手段7dへ出力する。送信制御手段7dは、情報制御手段8より出力されたマルチメディア情報のブロックを暗号化実行手段7b又は7cに出力し、暗号化実行手段7b、7cにより暗号化されたマルチメディア情報を受信手段4へ送信する。

【0041】受信手段4は、復号方式変更手段4a、復号実行手段4b、4c及び受信制御手段4dから構成されている。復号方式変更手段4aは、暗号方式送信手段8bにより送信された新たな復号手段に基づいて、受信手段4で使用する復号実行手段4b、4cを切り替える。復号実行手段4b、4cは、暗号方式送信手段8b

から送信された復号手段を実行するものであり、受信制御手段4dから出力されるデータを復号して、その結果を受信制御手段4dへ出力する。受信制御手段4dは、送信制御手段7dより出力された暗号化マルチメディア情報を復号実行手段4b又は4cに出力し、復号実行手段4b、4cにより復号されたマルチメディア情報を実行制御手段3へ送信する。

【0042】次に、動作について、図11のフローチャートに基づいて説明する。暗号方式送信手段8bは、暗号方式決定手段8aにより決定された暗号化鍵と暗号化手段を暗号方式変更手段7aへ送信する(ステップS20)。暗号方式変更手段7aは、受信した暗号化鍵と暗号化手段を暗号化実行手段7bへ出力し、暗号化実行手段7bを使用して暗号化するように設定する(ステップS21)。暗号方式送信手段8bは、復号鍵と復号手段受信手段4の復号方式変更手段4aへ送信する(ステップS22)。復号方式変更手段4aは、受信した復号鍵と復号手段を復号実行手段4bへ出力し、復号実行手段4bを使用して復号するように設定する(ステップS23)。

【0043】情報制御手段8は、マルチメディア情報をブロックに分割し、送信制御手段7dへブロックを送信する(ステップS24)。送信制御手段7dは、受信したブロックを、暗号化実行手段7bへ出力する(ステップS25)。暗号化実行手段7bは、ステップS21で出力された暗号化鍵と暗号化手段を使用してブロックを暗号化し、送信制御手段7dへ出力する(ステップS26)。送信制御手段7dは、暗号化されたブロックをネットワーク5を経由して受信制御手段4dへ送信する(ステップS27)。

【0044】受信制御手段4dは、ネットワーク5から暗号化されたマルチメディア情報のブロックを受信すると、復号実行手段4bへ出力する(ステップS28)。復号実行手段4bは、ステップS23で出力された復号鍵と復号手段を使用して暗号化ブロックを復号し、受信制御手段4dへ出力する(ステップS29)。受信制御手段4dは、復号したブロックを実行制御手段3へ送信する(ステップS30)。

【0045】次に、マルチメディア情報の実行中に暗号方式を変更する場合の動作を、図12のフローチャートに基づいて説明する。情報制御手段8は、現在使用している暗号方式が変更になると、マルチメディア情報のブロックの送信制御手段7dへの送信を停止する(ステップS40)。暗号方式送信手段8bは、暗号方式決定手段8aにより決定された変更後の暗号化鍵と暗号化手段を暗号方式変更手段7aへ送信する(ステップS41)。暗号方式変更手段7aは、受信した暗号化鍵と暗号化手段を暗号化実行手段7cへ出力し、次に受信するブロックは暗号化実行手段7cを使用して暗号化するように設定する(ステップS42)。暗号方式送信手段8

bは、暗号方式決定手段8aにより決定された変更後の復号鍵と復号手段を復号方式変更手段4aへ送信する(ステップS43)。復号方式変更手段4aは、受信した復号鍵と復号手段を復号実行手段4cへ出力し、次に受信する暗号化ブロックは復号実行手段4cを使用して復号するように設定する(ステップS44)。

【0046】情報制御手段8は、送信の停止を解除し、マルチメディア情報をブロックに分割し、送信制御手段7dへブロックの送信を再開する(ステップS45)。送信制御手段7dは、受信したブロックを暗号化実行手段7cへ出力する(ステップS46)。暗号化実行手段7cは、ステップS42で出力された変更後の暗号化鍵と暗号化手段を使用して、ブロックを暗号化し、送信制御手段7dへ出力する(ステップS47)。送信制御手段7dは、暗号化されたブロックをネットワーク5を経由して受信制御手段4dへ送信する(ステップS48)。

【0047】受信制御手段4dは、ネットワーク5から暗号化されたマルチメディア情報のブロックを受信すると、復号実行手段4cへ出力する(ステップS49)。復号実行手段4cは、ステップS42で出力された復号鍵と復号手段を使用して、ブロックを復号し、受信制御手段4dへ出力する(ステップS50)。受信制御手段4dは、復号したブロックを実行制御手段3へ送信する(ステップS51)。

【0048】以上のよう、この実施の形態によれば、使用する暗号方式を動的に変更することができるので、マルチメディア情報サーバに暗号方式を追加する場合に、システムを構成するハードウェアを変更する必要が無いという効果がある。

【0049】なお、この実施の形態では、暗号方式決定手段8aが新たな暗号方式を決定し、暗号方式送信手段8bは、新たな暗号方式に基づいて、鍵生成手段、暗号化手段及び復号手段を送信する形態を示したが、暗号方式決定手段8aが暗号方式送信手段8bの機能を有し、新たな暗号方式に対応する各手段を送信するように構成することも出来る。

【0050】この実施の形態では、図10に示したように、送信手段7内の暗号化実行手段7b、7c、及び、受信手段4内の復号実行手段4b、4cは、2つに限らず、2つ以上であっても良い。一度使用した暗号化方式は、暗号化実行手段7b、7c及び復号実行手段4b、4cに保存されていて、再度同じ暗号方式が使用されるときに、新しい暗号化鍵を暗号化実行手段7b、7cへ出力し、新しい復号鍵を復号実行手段4b、4cへ出力して、暗号化実行手段7b、7c内にある暗号化手段と、復号実行手段4b、4c内にある復号手段を再使用する。

【0051】また、暗号化実行手段7b、7c、又は、復号実行手段4b、4cが既に使用中で、未使用のものがないときは、使用頻度の低い暗号化実行手段7b、7

c、又は、復号実行手段4b、4cを使用するように制御する。

【0052】実施の形態7。実施の形態7は、図13に示すように、暗号化されたマルチメディア情報14bのブロックと、その暗号化に使用した暗号方式の暗号方式番号14aとによって構成される送信データ14を作成するものである。システムの構成は、実施の形態6で説明した図10のものと同様であるが、送信制御手段7dと受信制御手段4dの処理が異なる。送信制御手段7dは、図13に示した送信データを作成し、ネットワーク5を介して受信制御手段4dへ送信し、これを受信した受信制御手段4dは、暗号化されたマルチメディア情報14bを復号する復号手段を、暗号方式番号14aにより決定し、復号実行手段4b又は復号実行手段4cのいずれかに復号を実行させる。

【0053】実施の形態8。図14は、実施の形態8のマルチメディア情報システムの構成図である。図において、15はマルチメディア情報を実行するための複数の手段を実行方式番号とともに蓄積している実行方式データベースである。ユーザ情報データベース9は図2に示すものであり、マルチメディア情報データベース10は図3に示すものである。実行制御手段3は、実行情報制御手段3aと実行手段3bとから構成されている。実行手段3bは、受信手段4により復号されたマルチメディア情報を実行し、実行結果を出力手段2に送信する。実行情報制御手段3aは、一定時間間隔で、マルチメディア情報を実行している時の実行情報と、入出力手段2により出力されたユーザの要求とをマルチメディア情報サーバ6に送信する。実行情報には、ユーザ登録番号9b、実行中のマルチメディア情報番号10b、現在までのマルチメディア情報の実行の累積時間が含まれている。情報制御手段8は、制御手段8dとマルチメディア情報送信手段8eとから構成されている。制御手段8dは、実行情報制御手段3aにより送信されたマルチメディア情報の実行情報を受信してその情報を解析し、マルチメディア情報送信手段8eを制御する。マルチメディア情報送信手段8eは、マルチメディア情報データベース10からマルチメディア情報を取得し、送信手段7へ送信する。送信手段7は、マルチメディア情報を暗号化して受信手段4へ送信する。

【0054】次に、マルチメディア情報の実行を開始するまでの動作を図15のフローチャートに基づいて説明する。ユーザが一つのマルチメディア情報を選択すると、実行情報制御手段3aがユーザ登録番号9bとマルチメディア情報番号10bとを制御手段8dへ送信する(ステップS60)。制御手段8dは、ユーザ登録番号9bを検索条件としてユーザ情報データベース9からユーザの契約情報レコード9aを取り出し、契約タイプ9eから、要求のあったマルチメディア情報を実行可能であるか、また、要求の合った日時で実行が開始できるか

判定する(ステップS61)。制御手段8dは、マルチメディア情報の実行開始が可能であると判定すると、マルチメディア情報番号10bを検索条件としてマルチメディア情報データベース10からマルチメディア情報レコード10aを取り出し、実行方式番号10dを取得する(ステップS62)。次に、制御手段8dは、実行方式番号10dを検索条件として、実行方式データベース15から実行手段を取り出し、実行情報制御手段3aへ送信する(ステップS63)。実行情報制御手段3aは、受信した実行手段を実行手段3bへ出力する(ステップS64)。制御手段8dは、マルチメディア情報送信手段8eへマルチメディア情報番号10bを出力する(ステップS65)。マルチメディア情報送信手段8eは、マルチメディア情報番号10bを検索条件としてマルチメディア情報データベース10からマルチメディア情報レコード10aを取り出し、ブロックに分割して送信手段7へ送信する(ステップS66)。

【0055】送信手段7は受信したブロックを暗号化し、ネットワーク5を経由して、受信手段4へ送信する(ステップS67)。受信手段4は受信したブロックを復号して、実行手段3bへ送信する(ステップS68)。実行手段3bは、実行準備が終了したメッセージを入出力手段2へ出力する(ステップS69)。ユーザは入力手段2から、マルチメディア情報の実行開始を入力する(ステップS70)。実行情報制御手段3aは、実行開始の指示を受け取ると、マルチメディア情報の実行の開始のメッセージを制御手段8dへ送信し、実行の累積時間の計数を開始する(ステップS71)。制御手段8dは、マルチメディア情報の実行の開始のメッセージを受信すると、マルチメディア情報送信手段8eへ送信開始メッセージを出力する(ステップS72)。

【0056】次に、マルチメディア情報の実行中の動作を図16のフローチャートに基づいて説明する。マルチメディア情報送信手段8eは、マルチメディア情報番号10bを検索条件としてマルチメディア情報データベース10からマルチメディア情報を取り出してブロックに分割し、送信手段7へ送信する(ステップS80)。制御手段8dは、マルチメディア情報の実行の累積時間の計数を開始し、実行情報の受信を待つ(ステップS81)。送信手段7は、マルチメディア情報のブロックを暗号化し、ネットワーク5を経由して、受信手段4へ送信する(ステップS82)。受信手段4は、受信したブロックを復号し、実行手段3bへ送信する(ステップS83)。実行手段3bは、受信手段4からマルチメディア情報を受信すると、マルチメディア情報を実行し、実行結果を入出力手段2へ出力する(ステップS84)。

【0057】ステップS80～S84の動作を繰り返しているときに一定時間が経過すると(ステップS85)、実行情報制御手段3aは、現在までのマルチメディア情報の実行の累積時間をセットした実行情報を制御

手段8dに送信する(ステップS86)。制御手段8dは、制御手段8dが計数した実行の累積時間と実行情報にセットされている累積時間との差の絶対値を計算し、その差の絶対値が制御手段8dが保有している閾値の範囲を超えているかをチェックし(ステップS87)、超えている場合は(ステップS88)、契約タイプ9eに一致しない不正な実行が検出されたと判断し、送信の停止を示すメッセージをマルチメディア情報送信手段8eへ出力する(ステップS88)。マルチメディア情報送信手段8eはマルチメディア情報の送信を中止する(ステップS89)。

【0058】以上のように、この実施の形態によれば、マルチメディア情報の実行累積時間を契約タイプに基づいてチェックし、所定の時間を超えているときには送信を停止するので、マルチメディア情報の実行中に、契約条件に違反する不正なマルチメディア情報の実行を防止する効果がある。

【0059】実施の形態9、図17は、実施の形態9のマルチメディア情報システムの構成図である。図において、8fは実行情報を実行情報制御手段3aから送信するタイミングを制御手段8dからの要求で決定する実行情報送信方式決定手段である。

【0060】次に、動作について説明する。ユーザが一つのマルチメディア情報を選択すると、実行情報制御手段3aがユーザ登録番号9bとマルチメディア情報番号10bを制御手段8dへ送信する。制御手段8dは、ユーザ情報データベース9aからユーザ登録番号9bを検索条件として、ユーザの契約情報レコード9aを取り出し、契約タイプ9eを実行情報送信方式決定手段8fへ出力する。実行情報送信方式決定手段8fは、実行情報制御手段3aで使用できる実行情報送信方式の番号リストを内部に持っており、契約タイプ9eからリストの中の一つを選択し、選択した方式の方式番号を制御手段8dへ出力する。制御手段8dは、方式番号を実行情報制御手段3aへ送信する。実行情報制御手段3aは、方式番号を受信すると、実行情報を方式番号の実行情報送信方式に基づいて、制御手段8dへ送信する。

【0061】なお、実行情報の送信方式は、情報実行中にユーザの要求があった時のみ実行情報を送信する方式、あるいは、一定時間間隔で実行情報を送信する方式、あるいは、不規則な時間間隔で実行情報を送信する方式などがある。

【0062】以上のように、この実施の形態によれば、マルチメディア情報サーバへ実行情報を送信する方式を変更することにより、実行情報を送る時間にユーザおよび第三者が盗聴しうる実行情報を送信することができなくなるので、不正なマルチメディア情報の実行を防止する効果がある。

【0063】実施の形態10、図18は、実施の形態10におけるユーザ情報データベースの構成図であり、図

2に示したユーザ情報データベースに対して、マルチメディア情報番号9f、9hとマルチメディア実行制御情報9g、9iとを追加し、ユーザがサービスを契約しているマルチメディア情報の番号と実行制御情報とを保持している。この実施の形態のシステム構成は、図14に示したものと同様である。

【0064】次に、動作について説明する。ユーザが一つのマルチメディア情報を選択すると、実行情報制御手段3aがユーザ登録番号9bとマルチメディア情報番号10bを制御手段8dへ送信する。制御手段8dは、ユーザ情報データベース9からユーザ登録番号9bを検索条件として、ユーザの契約情報レコード9aを取り出し、その中のマルチメディア情報番号9f、9hに、ユーザが要求しているマルチメディア情報番号10bが含まれているか否かを確認する。制御手段8dは、ユーザが要求している番号を見つくと、マルチメディア情報番号9f、9hに対応するマルチメディア実行制御情報9g、9iに基づいて、マルチメディア情報の実行の開始が可能であるか否かを判定する。ユーザが要求している番号がない場合は、契約タイプ9eに基づいて、要求のあったマルチメディア情報を実行可能であるか否か、また、要求のあった日時で実行の開始が可能であるか否かを判定する。

【0065】マルチメディア情報の実行中にユーザの制御要求が発生すると、実行情報制御手段3aはその要求を実行情報として、制御手段8dへ送信する。制御手段8dは、マルチメディア実行制御情報9g、9iに基づいて、この要求が実行可能であるか否かを判定する。可能であると判定されれば、実行情報制御手段3aへ実行可能であるメッセージを送信する。実行情報制御手段3aは、実行手段3bをユーザの要求に基づいて制御する。不可能であると判定されれば、実行情報制御手段3aへ実行不可であるメッセージを送信する。実行情報制御手段3aは、入出力装置1へユーザの要求は破棄されたことを示すメッセージを出力する。

【0066】以上のように、この実施の形態によれば、ユーザ情報データベース中にユーザが契約しているマルチメディア情報の実行制御情報を格納し、この実行制御情報に基づいてマルチメディア情報を実行しているか否かを判別し、マルチメディア情報の送信を制御するので、契約条件に違反する不正なマルチメディア情報の実行を防止する効果がある。

【0067】実施の形態11. 図19は、実施の形態11におけるマルチメディア情報データベースの構成図であり、図3に示したマルチメディア情報データベースに対して、マルチメディア情報の実行を制御する実行制約条件10eを追加している。この実施の形態のシステム構成は、図14に示したものと同様である。

【0068】次に、動作について説明する。ユーザが一つのマルチメディア情報を選択すると、実行情報制御手

段3aがユーザ登録番号9bとマルチメディア情報番号10bを制御手段8dへ送信する。制御手段8dは、ユーザ登録番号9bを検索条件として、ユーザ情報データベース9からユーザの契約情報レコード9a中のユーザの契約タイプ9eを取り出す。また、制御手段8dは、マルチメディア情報番号10bを検索条件として、マルチメディア情報データベース10からマルチメディア情報レコード10a中の実行制約条件10eを取り出し、ユーザの契約タイプ9eが実行制約条件10eに含まれているか否かを確認する。含まれている場合は、契約タイプ9eから、要求のあったマルチメディア情報を実行可能であるか否か、また、要求の合った日時で実行の開始が可能であるか否かを判定する。含まれていない場合は、ユーザからの要求を破棄し、ユーザからの要求が破棄されたことを示すメッセージを実行情報制御手段3aへ送信する。実行情報制御手段3aは、入出力装置1へユーザの要求が破棄されたことを示すメッセージを出力する。

【0069】以上のように、この実施の形態によれば、マルチメディア情報データベース中にマルチメディア情報を実行するための実行制約条件を格納し、この実行制約条件に基づいてマルチメディア情報を実行しているか否かを判別し、マルチメディア情報の送信を制御するので、契約条件に違反する不正なマルチメディア情報の実行を防止する効果がある。

【0070】

【発明の効果】以上のように、請求項1記載の発明によれば、マルチメディア情報を暗号化する暗号化手段と、この暗号化手段により暗号化されたマルチメディア情報を復号する復号手段とを、ユーザとの契約情報に基づいて決定することにより、ユーザ毎に暗号方式を変更しているので、第三者は暗号方式の推測が困難であるため、マルチメディア情報への不正なアクセスが排除できるという効果がある。

【0071】請求項2記載の発明によれば、複数の暗号化手段と複数の復号手段とを記憶する暗号方式記憶手段を備え、暗号化手段と復号手段とをユーザとの契約情報に基づいて決定することにより、ユーザ毎に暗号方式を変更しているので、第三者は暗号方式の推測が困難であるため、マルチメディア情報への不正なアクセスが排除できるという効果がある。

【0072】請求項3記載の発明によれば、暗号化マルチメディア情報を送信する送信手段は、複数の暗号化手段を記憶する暗号方式記憶手段を備え、暗号化マルチメディア情報を復号する受信手段は、複数の復号手段を記憶する復号方式記憶手段を備えたので、復号手段をサーバからクライアントに送信する必要が無いため、復号手段の送信時間分を短縮できるという効果がある。

【0073】請求項4記載の発明によれば、暗号化手段の使用可能な地域を示す地域情報を記憶する地域情報記

憶手段を備え、ユーザとの契約情報と地域情報とに基づいて暗号化手段と復号手段とを決定するので、使用できる暗号方式が地域によって異なる場合にも、暗号方式を選択できるという効果がある。

【0074】請求項5記載の発明によれば、サーバの送信手段は、実行中でない暗号化実行手段に暗号化を実行させる暗号方式変更手段を備え、クライアントの受信手段は、実行中でない復号実行手段に復号を実行させる復号方式変更手段を備えたことにより、使用する暗号方式を動的に変更することができるので、暗号方式を追加する場合に、システムを構成するハードウェアを変更する必要が無いという効果がある。

【0075】請求項6記載の発明によれば、暗号化マルチメディア情報の送信データ中に使用した暗号化手段の種別を格納することにより、送信データから暗号方式を知ることができるので、暗号方式をクライアントへ通知する必要が無く、時間が短縮できるという効果がある。

【0076】請求項7記載の発明によれば、クライアント側でのマルチメディア情報の実行状態を示す実行情報をユーザとの契約情報と照合し、契約に基づいてマルチメディア情報を実行しているか否かを判別するので、契約条件に違反する不正なマルチメディア情報の実行を防止する効果がある。

【0077】請求項8記載の発明によれば、クライアントからサーバへの実行情報送信方式をユーザとの契約情報に基づいて決定することにより、実行情報を送る時間に盗聴し虚の実行情報を送信することができなくなるので、契約条件に違反する不正なマルチメディア情報の実行を防止する効果がある。

【0078】請求項9記載の発明によれば、ユーザ情報記憶手段中にユーザが契約しているマルチメディア情報の実行制御情報を格納し、この実行制御情報に基づいてマルチメディア情報を実行しているか否かを判別し、マルチメディア情報の送信を制御するので、契約条件に違反する不正なマルチメディア情報の実行を防止する効果がある。

【0079】請求項10記載の発明によれば、マルチメディア情報記憶手段中にマルチメディア情報の実行を制約する実行制約条件を格納し、この実行制約条件に基づいてマルチメディア情報を実行しているか否かを判別し、マルチメディア情報の送信を制御するので、契約条件に違反する不正なマルチメディア情報の実行を防止する効果がある。

【図面の簡単な説明】

【図1】 実施の形態1のマルチメディア情報システムの構成図である。

【図2】 ユーザ情報データベースの構成図である。

【図3】 マルチメディア情報データベースの構成図である。

【図4】 暗号方式データベースの構成図である。

【図5】 実施の形態1のマルチメディア情報システムの動作を示すフローチャートである。

【図6】 実施の形態2のマルチメディア情報システムの構成図である。

【図7】 実施の形態3のマルチメディア情報システムの構成図である。

【図8】 実施の形態4のマルチメディア情報システムの構成図である。

【図9】 実施の形態5の暗号方式データベースの構成図である。

【図10】 実施の形態6のマルチメディア情報システムの構成図である。

【図11】 実施の形態6のマルチメディア情報システムの動作を示すフローチャートである。

【図12】 実施の形態6のマルチメディア情報システムにおける暗号方式を変更する場合の動作を示すフローチャートである。

【図13】 実施の形態7におけるマルチメディア情報サーバの送信データの構成図である。

【図14】 実施の形態8のマルチメディア情報システムの構成図である。

【図15】 実施の形態8のマルチメディア情報システムの動作を示すフローチャートである。

【図16】 実施の形態8のマルチメディア情報システムにおけるマルチメディア情報実行中の動作を示すフローチャートである。

【図17】 実施の形態9のマルチメディア情報システムの構成図である。

【図18】 実施の形態10におけるユーザ情報データベースの構成図である。

【図19】 実施の形態11におけるマルチメディア情報データベースの構成図である。

【図20】 従来のマルチメディア情報システムの概略構成図である。

【図21】 従来のマルチメディア情報システムにおけるメタデータの構成図である。

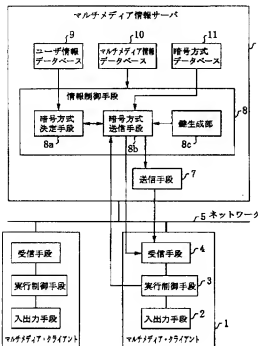
【符号の説明】

1 マルチメディア・クライアント、2 入力手段、3 実行制御手段、3a 実行情報制御手段、3b 実行手段、4 受信手段、4a 復号方式変更手段、4b、4c 復号実行手段、4d 受信制御手段、5 ネットワーク、6 マルチメディア情報サーバ、7 送信手段、7a 暗号方式変更手段、7b、7c 暗号化実行手段、7d 送信制御手段、8 情報制御手段、8a 暗号方式決定手段、8b 暗号方式送信手段、8c 鍵生成部、8d 制御手段、8e マルチメディア情報送信手段、8f 実行情報送信方式決定手段、9 ユーザ情報データベース、9a 契約情報レコード、9b ユーザ登録番号、9c 氏名、9d 住所、9e 契約タイプ、9f マルチメディア情報番号、9g マルチメ

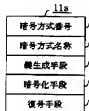
イ実行制御情報、9h マルチメディア情報番号、9i マルチメディア実行制御情報、10 マルチメディア情報データベース、10a マルチメディア情報レコード、10b マルチメディア情報番号、10c マルチメディア情報の名称、10d 実行方式番号、10e 実行制約条件、10f マルチメディア情報、11 暗号方式データベース、11a 暗号方式レコード、1

1b暗号方式番号、11c 暗号方式の名称、11d 鍵生成手段、11e 暗号化手段、11f 復号手段、11g 使用可能地域情報、12 復号手段データベース、13 暗号化手段データベース、14 送信データ、14a 暗号方式番号、14b 暗号化されたマルチメディア情報、15 実行方式データベース。

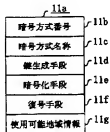
【図1】



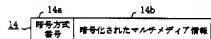
【図4】



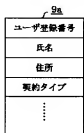
【図9】



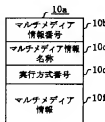
【図13】



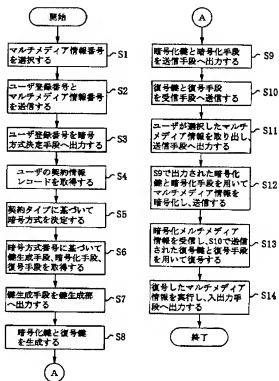
【図2】



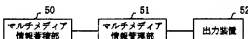
【図3】



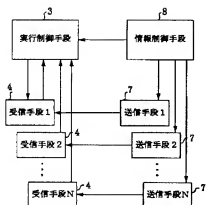
【図5】



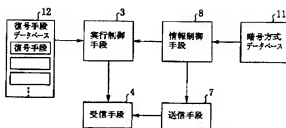
【図20】



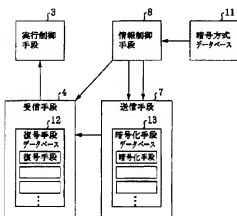
【図6】



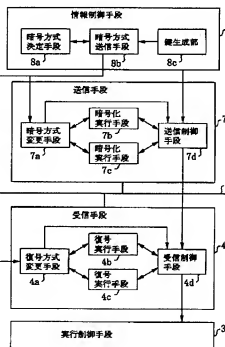
【図7】



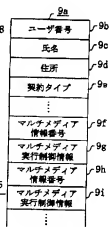
【図8】



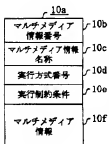
【図10】



【図18】



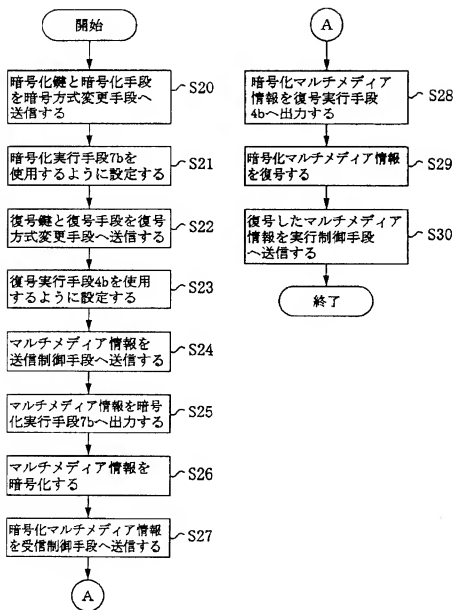
【図19】



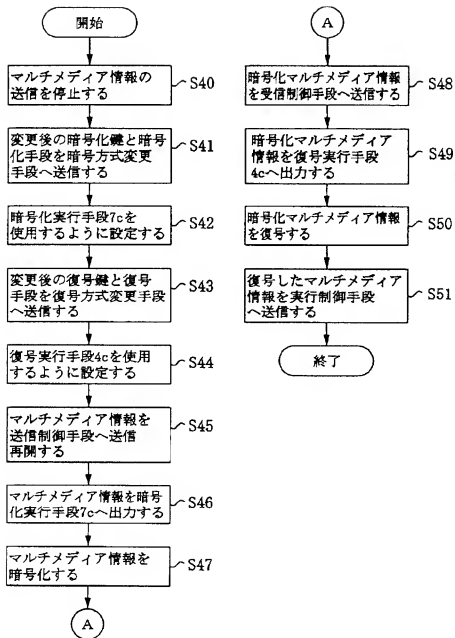
【図21】



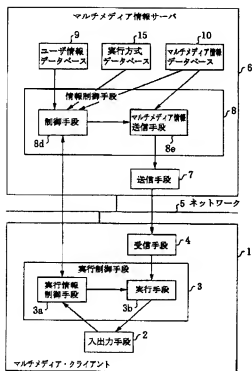
【図11】



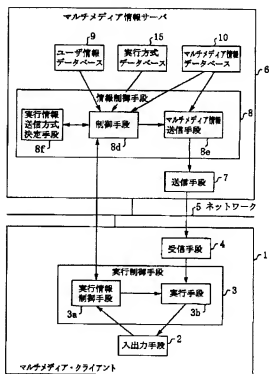
【図12】



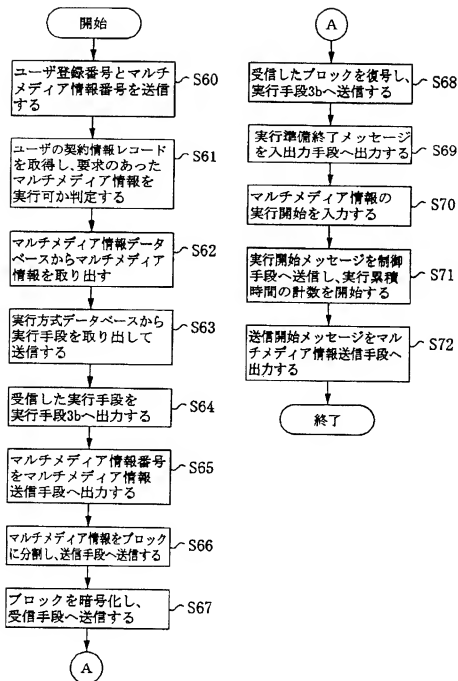
【図14】



【図17】



【図15】



【図16】

